CLICK TO MEET™
CONFERENCE SERVER

User Guide

RADVISION Ltd.

Proprietary Information

The information contained in this online document is subject to change without notice.

RADVISION Ltd. makes no warranty of any kind with regard to this written material. RADVISION Ltd. assumes no responsibility for any errors that may appear in this document or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

Click to Meet, Click to Meet Conference Server and CU-SEEME are trademarks of RADVISION Ltd.

Elemedia is a trademark of Lucent Technologies, Inc.; Java is a trademark of Sun Microsystems, Inc.; Microsoft, Windows, NetMeeting, Office Communicator, Live Communications Server, Internet Explorer, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries; Linux is a trademark of Linus Torvalds; Red Hat is a registered trademark or trademark of Red Hat, Inc. in the United States and/or other countries.

All other product names used in this document are trademarks or registered trademarks of their respective manufacturers.

This product includes software developed by the Apache Software Foundation (http://www.apache.org)

This product includes software developed by Borland Software Corp.

This product includes software developed by The Legion Of The Bouncy Castle Copyright © 2000 – 2004 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

This product includes code licensed from RSA Security, Inc.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

This product includes Agere™ Codec software technology from Lucent Technologies, Inc. Copyright © 1995-2001 Lucent Technologies, Inc.

Contains iLBC codec from Global IP Sound Inc. (http://www.globalipsound.com). Copyright © 1999-2006 Global IP Sound Inc.

ACE™, TAO™ and CIAO™ are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved.

Portions Copyright © 1996 by the University of Southern California
Portions Copyright © 2000 Alexandria Software Consulting
Portions Copyright © 1995-2003 Jean-loup Gailly and Mark Adler
Portions Patent 1990-2002 DSP Group, Inc.
Portions Patent 1990-2002 SIPRO LAB TELECOM, INC
Portions Patent 1990-2002 NEC Corporation
Portions Patent 1990-2002 Nokia Corporation
Portions Patent 1990-2002 Nortel Corporation
Portions Copyright © 1998-2006 The OpenSSL Project. All rights reserved.
Portions Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

Copyright © 1999-2006 RADVISION Ltd. All Rights Reserved.

Publication Date: October, 2006

Product Version 7.6.000 Rev. 01

Table of Contents

PROPRIETARY INFORMATION 2

Table of Contents 3

Before You Begin 10

What is the Click to Meet Conference Server? 10

Product Components 10

Product options 11

About the T.120 Standard 12

About the H.323 Standard 13

The H.323 Standard: Gatekeeper Functionality 13

Getting Started - The Conference Server Administrator Web Pages 15

The Help System 16

Log Out Button 16

The Log Display Window 16

The Network 17

Working with Conference Server Domain Members 17

Adding a Conference Server to the Conference Server Domain 17

Configuration Settings 17

Gatekeeper Settings 18

Optional Gatekeeper terminal aliases for Conference Server 18

H.323 Domain Name 19

Conference Server E.164 Address Prefix 19

No Gatekeeper 19

Use the Conference Server Gatekeeper 20

Ignore discovery requests from the following IP ranges 20

Conference Server Endpoint Identifier Suffix 20

Use a Third-Party Gatekeeper 20

Removing a Conference Server from the Domain 21

Shutting Down the Conference Server 21

Working with Firewalls 21

Enabling E-Mail 23

Synchronizing Conference Server Domain Members 24

Editing Conference Server Settings 25

Working with the Conference Administrator database 26

Defining Your Conference Administrator Database 26

Managing Organizations in the Conference Administrator Database 27

Adding an Organization Record to the Conference Administrator database 27

Editing an Organization Record in the Conference Administrator database 27

Removing an Organization Record from the Conference Administrator database 27

Initializing the Conference Administrator Database 28

Backing up the Conference Administrator Database 28

Adding User Records to the Conference Administrator Database 28
User Identifier Fields 29
Searching User Records in the Conference Administrator Database....30
Editing User Records in the Conference Administrator Database....30
Copying User Records in the Conference Administrator Database....31
Removing User Records from the Conference Administrator Database 31
Conference Server T.120 Features 32
Data Conferencing with the Conference Server T.120 Server....32
About T.120 Transport Security 32
GSS-API and SSL/TLS 33
Digital Certificate....33
The T.120 Configuration File....33
Enabling the T.120 Security Feature....34
T.120 Throughput Enforcement 35
Querying Status of T.120 Security 36
Joining a T.120 Conference....36
Inviting a User into a T.120 Conference....36
Linking T.120 Servers 37
The User Authentication Page and T.120 37
Configuring T.120 Conferences 37
Enabling T.120 for H.323 conferences....37
Enabling T.120 for non-H.323 conferences....38
H.323 and the Conference Server....39
Hosting H.323 Conferences 39
Receiving video and audio....39
Default video switching 40
The H.323 VideoSwitcher Applet 40
The Continuous Presence Mode Option 40
Time-based Switching....41
Managing Bandwidth with the Conference Server....42
Automatic Bandwidth Controls 42
Automatic Bandwidth Detection 42
Automatic Bandwidth Pruning....42
Manual Bandwidth Controls 42
Setting Conference-Specific Limits 43
Setting Server-Wide Limits....43
Setting up Multiple-Server Conferences 43
Participating in Conferences 45
Selecting a Conference 45
Selecting a Conference Through a Gatekeeper....45
H323-ID Terminal Alias....45
E.164 Terminal Alias....46
Selecting a Conference Through the T.120-Based Server....46
Selecting a Conference Through the User Authentication Web Page....46
Selecting a Conference Through Default Conference Routing 47
Selecting a Conference Through the CallOut Applet 47

Entering a Conference Password 47
Scheduling 48
Always enabled 48
Always disabled 48
Limit access to scheduled time 48
Creating and Configuring Conferences 49
The Conferences Area 49
Viewing Available Conferences 49
Adding a Conference 51
Basic Settings 52
Conference ID 52
Private 52
Conference Name 53
Conference Greeting 53
Conference Attributes 53
Video (default = on) 53
Audio (default = on) 53
Chat (default = on) 53
H.323 w/T.120 (default = off) 53
SIP (default = off) 54
People and Content 54
Broadcast Mode 54
Normal 54
Broadcast 54
Maximum Participants 55
Optional/Advanced Settings 55
Template Conference 56
Conference Owner Information 56
Conference Owner 56
E-mail Address 56
Phone Number 56
Conference URL 57
Description 57
Conference Password 57
Scheduling 57
Start Date 57
Start Time 57
Duration 57
Repeat conference 58
Bandwidth Controls 58
Maximum Send Rate 58
Maximum Receive Rate 58
Time Limits 58
Bandwidth 59
Required Codecs 59
Time Limits 62
Disconnect participants after 62

Time limit disconnect time....62
Restrict Participant Message....62
Data Collaboration for Non-H.323 Conferences....62
User Authentication....62
Conference Server Authentication....62
IP-Based Authentication....62
Username/Password Authentication....63
RADIUS authentication....63
Audio / Video Codecs....63
Audio Codecs....63
Video Codecs....64
Audio Latency....65
Conference Aliases....65
Conference Nicknames....66
User-Defined Aliases....66
Unicast and Multicast....66
Self-Reflect....68
Root....68
Enable tracking....69
Streaming....70
H.263+ Annexes....70
Editing a Conference Configuration....70
Copying a Conference Configuration....71
Removing a conference....71
The Conference Server Layout Applet....73
Working with the Conference Server Layout Applet....73
The Mapping Area....73
The Toolbar....73
Selection Tool....73
Conference Server Tool....73
Multicast Tool....73
Uni-Directional Link Tool....73
Bi-Directional Link Tool....74
Top Provider Tool....74
Load Button....74
Save Button....74
Delete Button....74
Quit/Apply Button....74
Defining a Server Layout for Your Conference....74
Linking Data Streams....75
Multicast Linking....75
Port Numbers....75
Time to Live Value....76
Creating a Uni-Directional or Bi-Directional Link....76
Changing Linking Settings....77
One-Way Link....77
Two-Way Link....77

Multi-Conference Links 77
Keep-Alive Messages 78
Designating a Top Provider....78
Clearing the Mapping Area 78
Changing Layout Settings 78
Creating a Conference Server Layout Template....79
Editing an Existing Template....79
Deleting an Existing Template 79
Applying a Template to the Layout of a Conference....80
Avoiding Conference Server Layout Conflicts....80
Managing User Access to Conferences 82
The Users Area 82
Assigning Special Permissions 82
Administrator Permission 83
Moderator Permission....83
Conference Manager Permission....84
General User Permission....84
General User: Normal Permission....84
General User: Admit Permission....85
General User: Deny Permission....85
General User: Admitted-sender Permission....85
Conference Server's User Authentication Web Page 87
Accessing Conference Server's User Authentication Web Page 88
Customizing the User Authentication Web Page 90
User authentication 90
Monitoring Conferences....91
The Monitoring Area....91
Using the Monitoring Area as an Administrator....91
Using and Accessing the Monitoring Area as a Moderator....91
Monitoring Users 92
Disconnecting a User....94
Denying a User 95
Granting the Floor to a User....95
Revoking the Floor from a User 96
Setting/clearing Video Sources....97
Monitoring Dynamic Statistics for a Conference 97
Monitoring Dynamic Statistics for a Conference Server 98
Monitoring Gatekeeper Activity 98
Doing More with Conference Server 101
Administrative Server 101
Using Conference Server's Continuous Presence Mode applet....102
Using Conference Server's H.323 VideoSwitcher Applet 104
Using Conference Server's CallOut applet....106
Using Conference Server's MeetingPlanner Applet....108
Create a Template Conference....109

Create an Organization Record....110
Create a Conference Manager User Record....110
MeetingPlanner....111
Using MeetingPlanner with General User permission....112
Option: This conference is open to everyone....113
Option: This conference is password protected....113
Using MeetingPlanner with Conference Manager permission....114
Option: "This conference is open to everyone"....116
Option: "This conference is password protected"....116
Option: "This conference is limited to specific participants"....117
Providing Conference Server User Tools to client end users....119
Historical statistics....119
Log file name....119
Log interval....119
Line limit....119
Backup interval....120
Interfacing with Third-Party Billing Systems....120
Understanding Conference Server's Billing Architecture....120
Session Data....121
User Authentication....122
Defining Your RADIUS Server....122
Enabling Streaming Media....123
Enable the Streaming of a Conference Server Conference....123
Additional Information on Installing Conference Server's Streaming Drivers....124
Now issue the stream-media command....124
Display a message before Conference Server sends video....125
Using QuickTime Streaming on the Conference Server....125
Creating an SDP file....127
SDP Creation Tool....129
Installation....129
Using the SDP Page....130
Login and Logout....131
Using SNMP with the Conference Server....131
Where is the service configuration file?....131
How do you modify the service configuration file?....131
SNMP Support....132
Configuring the SNMP Agent from a Windows System....132
Configuring the SNMP Agent from a Unix System....132
The SNMPD.conf file....133
Using SOAP with the Conference Server....134
Working with Conference Server's Historical Statistics....137
Simple Cascading....138
Setting up Simple Cascading....139
What if there are two servers registered to the same gatekeeper?....140
CORPORATE WEB SITE....141
TECHNICAL SUPPORT....141

THIRD-PARTY LICENSING 141

INDEX 144

Before You Begin

RADVISION frequently updates the Click to Meet Conference Server documentation. Please visit the documentation section of our Web site at http://support.clicktomeet.com. Download the latest version of this User Guide from the Web site to ensure that you have the most up-to-date information.

What is the Click to Meet Conference Server?

The Click to Meet Conference Server is a multipoint conferencing unit. It delivers multimedia group conferences across IP-based networks. It allows participants using a variety of videoconferencing clients to work, learn, and socialize in a multipoint conferencing environment. It also:

- Allows groups of users with networked personal computers or conferencing systems to interact in real-time, sharing any combination of audio, video, text, and data.
- Enables administrators to control the use of multimedia communications on their network, offering bandwidth control and optimization, security, conference administration, and monitoring services.
- Offers multipoint conferencing services to H.323 standards-based clients, thus allowing participants using a variety of videoconferencing clients to work, learn, and socialize in a mulitpoint conferencing environment.
- Offers easy integration into existing network environments. It runs on Microsoft® Windows® 2000 Server™, Windows Server™ 2003, and Red Hat® Linux ® platforms and can be accessed from most computer platforms through a Web browser.
- Intelligently manages the amount of bandwidth required for group interaction, takes full advantage of IP Multicast technology, and facilitates billing and tracking with third-party systems.
- Can be purchased with add-on options that provide advanced functionality such as H.323 continuous presence conferences and integration with streaming media technologies.

Product Components

The Conference Server is made up of multiple software components that work together to provide a comprehensive solution for multimedia group conferences over IP networks. Before installing the software, it is helpful to understand what the major product components are and how they work together.

Videoconferencing Server

The videoconferencing server provides the core technology for the Conference Server product. It routes audio, video, and CUseeMe-protocol chat streams. It provides bandwidth control, security, conference configuration, user authentication, monitoring, and H.323 gatekeeper functionality.

T.120 Server

The T.120 server works in conjunction with the videoconferencing server to add document and application sharing to conferences (for clients that support the T.120

standard.) It installs automatically with the videoconferencing server.

Conference Administrator Web Pages

The Conference Administrator Web pages provide a browser-based interface for conference administration and users.

Conference Administrator Database

The Conference Administrator database keeps user authentication information. It installs with the Conference Administrator Web pages.

User Authentication Web Page

The User Authentication Web page facilitates user authentication, billing, and the routing of H.323 clients. It installs with the Conference Administrator Web pages.

Conference Server MeetingPlanner

The MeetingPlanner is a Java applet that allows end users to create and schedule conferences on their own. It installs with the Conference Administrator Web pages.

H.323 VideoSwitcher Applet

The H.323 VideoSwitcher Applet is a Java applet that allows H.323 end users to choose which participant to watch and listen to in an H.323 conference. It installs with the Conference Administrator Web pages.

Continuous Presence Mode Applet

The Continuous Presence Mode applet is a Java applet that allows a conference moderator or Conference Server administrator to control how video displays in each cell of an H.323 continuous presence video window. It installs with the Conference Administrator Web pages, **but only works if you have the license option.**

H.323 CallOut Applet

The CallOut applet is a Java applet that enables users to make callouts, or invitations, to potential conference participants. It installs with the Conference Administrator Web pages.

Conference Server User Tools

The Conference Server User Tools is a Windows-based desktop installer that you can provide to your end users. It provides shortcuts from the Windows **Start** menu for easy access to the User Authentication Web page, the MeetingPlanner, the H323 Video Switcher Applet, the Continuous Presence Mode Applet, and the CallOut Applet. The User Tools installer is not part of the product installation. It is located in the UserTools directory of your product CD.

Product options

You can purchase the Conference Server with the following options:

Video

The Video option is standard on Conference Server. It enables video for Conference Server conferences.

Additional Audio

The Additional Audio option enables expanded audio capabilities and additional codec support -- G.722 and G.729A -- for increased speech quality at reduced bandwidth requirements.

Continuous Presence Mode option

The Continuous Presence Mode option enables H.323 client endpoints to view multiple windows at the same time.

Streaming Media option for Microsoft® Windows® 2000

The Streaming Media option enables the Conference Server to distribute an audio/video stream from a conference for distribution to a large audience. It also records the conference for a permanent, easily-accessible record.

H.323

The H323 option enables H.323 users to participate and creates a matching T.120 data conference.

SIP

The SIP option allows Microsoft Windows XP SIP clients to participate in a conference.

Conference Client (Web option)

The Conference Client ™ automatically enables your desktop with rich media communication tools.

About the T.120 Standard

The T.120 standard is an open standard that provides a series of protocols and services for real-time, multipoint data communications. The International Telecommunications Union (ITU) established the T.120 standard to ensure interoperability between client applications from multiple vendors.

The T.120 standard facilitates two different levels of interoperability:

- The lower-level layers of the T.120 standard (T.122, T.123, T.124, and T.125) provide *network-level* interoperability. Network-level interoperability encompasses conference control and multipoint data transport.
- The upper-level layers (T.126, T.127, and T.128) provide *application-level* interoperability for specific conferencing applications. Application-level interoperability guarantees that client applications from different vendors can share information. Common conferencing applications include shared whiteboard (still image exchange and annotation), binary file transfer, and application sharing.

The Conference Server T.120 server facilitates network-level interoperability. It provides connection and control for T.120 client applications. However, it is important to note that most T.120 applications have not yet conformed to application-level T.120 standards. This is primarily because the application layers were developed and ratified much later than the network layers. This means that while all T.120 clients can connect to the same T.120 conference, only users with client applications that incorporate ***like*** data conferencing components can data conference with one another.

As vendors incorporate the application-level layers of the T.120 standard into their client applications, true interoperability will result. It is important to note that the T.120 standard is broad. Vendors may continue to choose which application layers to incorporate and which to leave out. For example, some T.120 clients support only shared whiteboard, while others may additionally support binary file transfer and application sharing.

The Conference Server T.120 server allows participants using T.120 clients to share data with like clients in any format that the client application supports. For example, if a T.120 client application has application sharing functionality, the participants using the client will be able to application share in a T.120 conference. Each client application may perform slightly differently with the Conference Server T.120 server.

Note: H.323 videoconferencing clients that incorporate Microsoft NetMeeting for data sharing can data share in a Conference Server videoconference.

About the H.323 Standard

As more computers become enabled for videoconferencing, interoperability becomes increasingly important. With users from around the globe communicating via hardware and software from a variety of manufacturers, industry standards are required to ensure interoperability. The Conference Server is a standards-based solution that provides multipoint conferencing services to H.323 standards-based clients. These clients include CU Web, CUseeMe Pro, and the Click to Meet Conference Client.

The H.323 standard serves as the "umbrella" for a suite of recommendations defined by the International Telecommunication Union (ITU). The H.323 standard defines videoconferencing over packet-switched (generally IP-based) networks such as local area networks (LANs) and the Internet. It covers both point-to-point and multipoint audio and video conferencing. In addition, the ITU has defined the T.120 standard to address the document sharing (data conferencing) portion of a multimedia conference.

The H.323 Standard: Gatekeeper Functionality

H.323 standards define several components of real-time multimedia communications over packet-based networks. These include:

Terminals	H.323 terminals provide real-time voice and, optionally, video and data communications. Any H.323-based videoconferencing client is an H.323 terminal.
Gatekeepers	H.323 gatekeepers are network-level administration servers. They provide call control services to H.323 endpoints (an endpoint can be a terminal, gateway, or multipoint control unit.)
Gateways	H.323 gateways provide translation between circuit-switched networks and packet-based networks, enabling H.323 endpoints to communicate with non-H.323 endpoints.
Multipoint Control Units (MCUs)	H.323 MCUs provide support for multipoint conferences between three or more endpoints. An MCU manages conference resources, negotiates capabilities between endpoints, and more.

The Conference Server is a multipoint control unit with an integrated H.323 gatekeeper. The Conference Server can register as an endpoint with its own local gatekeeper or with a third-party gatekeeper.

The services that gatekeepers provide include the following:

- **Address Translation -** Gatekeepers perform translation from alias-address to transport-address. Endpoints register one or more aliases with the gatekeeper. Other endpoints then query the gatekeeper for a desired alias. All Conference Server H.323 conferences

have registered aliases with the gatekeeper.

- **Admissions Control -** H.323 endpoints send RAS (Registration, Admission, Status) messages to the gatekeeper. The gatekeeper authorizes network access to these endpoints. When a terminal (videoconferencing client) sends a request to connect to a conference, the gatekeeper queries the Conference Server's existing authorization mechanisms to determine whether to admit the terminal.

  Only H.323 clients that support RAS messaging can register for call control services with the gatekeeper. Some clients do not support RAS and therefore cannot register with the gatekeeper. You can use the Telnet gk-route command to create an alias manually for H.323 clients without RAS capabilities. For more information, see the gk-route command in the **Conference Server Telnet Guide**.

- **Bandwidth Control -** Endpoints send requests for network bandwidth to the gatekeeper. The gatekeeper grants or denies these requests based on the sum of send and receive rates (for the conference or for the Conference Server, whichever is less.)

  Bandwidth management through a third-party gatekeeper is *advisory only*. A third-party gatekeeper cannot prevent an H.323 client from connecting to a conference based on aggregate bandwidth allocation for the zone. Clients must conform to the Conference Server bandwidth restrictions in order to connect to a conference.

- **Zone Management -** A gatekeeper is required to provide address translation, admissions control, and bandwidth control to all endpoints that register with it. The network administrator defines the rules under which endpoints can register with a gatekeeper. The Conference Server local gatekeeper allows administrators to specify IP addresses or subnets from which the gatekeeper does not accept registration requests.

  You can specify whether Conference Server uses the services of its local gatekeeper or those of a third-party gatekeeper. In the **Network** area of Conference Administrator Web pages, you can add a new domain member or edit the settings of an existing one. You can specify gatekeeper functionality for each Conference Server in your domain. For more information, see **Gatekeeper Settings**.

Getting Started - The Conference Server Administrator Web Pages

Once you start the Conference Server, you can manage all configuration, management, and monitoring through the Conference Administrator Web pages.

To access Conference Server through your Web browser:

1. Open your browser and enter the following URL (personalized with the IP address or domain name of the computer on which you installed the Conference Administrator Web pages):

   `http://<yourserver>:8080/cs/cs.html`

Note that <yourserver> is the IP address or the host name of the computer on which the Conference Administrator Web pages are located. For example, if you installed the Conference Administrator Web pages on a computer with IP address **100.1.1.1** and domain name **conference.radvision.com**, you could enter either of the following URLs:

```
http://100.1.1.1:8080/cs/cs.html
http://conference.radvision.com:8080/cs/cs.html
```

The Conference Server login page displays and prompts you for a username and password

Note: From a Windows computer, you can get to the login page directly by selecting **Conference Server Login** from the Conference Server group on the Windows **Start** menu.

2. In the **Username** field, enter **`Administrator`**. Be sure to use a capital A for the Administrator username.
3. In the Password field, enter **changeme**. Be sure to use all lowercase letters for the password.

   The Conference Server installs with this default username and password. To avoid unauthorized access, RADVISION strongly recommends that you change the username and password in the user database as soon as possible. For more information, see **Editing User Records**.
4. In the **Permission** field, select **Administrator** and click **OK**. The Conference Server main entry page displays.

   Selecting Administrator in the drop-down box gives you full administrative access to the Conference Server. For information on accessing the Conference Server as a **Moderator**, see **Accessing the Monitoring Area as a Moderator**.

The main entry page for the Conference Server links to five main areas:

- Network
- Conferences
- Users
- Monitoring
- Help

To access any of these five areas, click the appropriate button at the bottom of the Conference Server main entry page. Once you are past the main entry page, the navigation icons for each of the major areas display in a column on the left side of the browser window.

These navigation icons display throughout the Conference Server interface.

To go back to the main entry page, click the Conference Server icon at the top of the column of navigation icons. The main entry page also has a **Log Out** button.

The Help System

You can click the Help icon from anywhere within Conference Administrator Web pages. A second browser window opens which displays the Conference Server Help system. This allows you to have both the Help system and the Conference Administrator Web pages open at the same time.

The documentation for the Conference Server includes:

- Conference Server User Guide
- Conference Server Telnet Guide
- Conference Server Installation and Upgrade Guide
- Release Notes
- What's New

To be sure that you have the latest information, please visit the documentation section of the RADVISION Web site at http://support.clicktomeet.com.

Log Out Button

The **Log Out** button provides additional security. When you finish using the Conference Server, navigate to the entry page and click the Log Out button to end your browser session. When you finish a session by logging out, no other user can access the Conference Administrator Web pages from your system.

As an added security mechanism, the Conference Server times out browser sessions after a two-hour period of inactivity. You can avoid time outs by leaving your browser connected to a page that does automatic updates. In this case, the session remains open indefinitely.

The pages that do automatic updates are:

- Conferences page (top level)
- Conference Server Domain Members page in the Network area
- Monitor Users page in the Monitoring area

If you forget to log out when you leave the Conference Server interface, you can get back in as part of the previous session any time within the two-hour limit. You can then click the Log Out button to end the session.

The Log Display Window

The Log Display window shows the Conference Server configuration file at startup. It also records subsequent activity on the Conference Server. You can open or close this window at any time without affecting the operation of the Conference Server.

You can use a Telnet command to instruct Conference Server to write the log window information to a file called **cs.log** in the installation directory. For more information, see the log command in the **Conference Server Telnet Guide**.

The Network

Working with Conference Server Domain Members

The **Conference Server Domain Members** page displays a selection box with a list of Conference Servers currently associated with the domain. It also presents a button bar linking to tasks that you can perform. The Conference Servers are identified in the selection box by hostname, IP address, and operating status (that is, whether the Conference Server is running or stopped).

One Conference Server in the domain typically functions as the administrative server for the entire domain. The administrative server maintains the conference configuration file and propagates any changes to it to the other Conference Servers in the domain.

You must choose an administrative server during installation, but you can change your selection later. If you install a single Conference Server, that server must act as its own administrative server. The administrative server is denoted by an asterisk (*) after its name.

Adding a Conference Server to the Conference Server Domain

When you add a Conference Server to a domain, you set up communication between the new server and all the other Conference Servers in the network. You can manage this communication from the Administrator Web pages.

You must install the Conference Server and it must be operational before you can add it to a domain. During installation, you define server-wide settings. Note that a new Conference Server in a domain must reference the administrative server in the same domain. For more information, see the Conference Server Installation and Upgrade Guide.

To add a Conference Server to your Conference Server domain:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page displays.
2. Click the **Members** button. The **Conference Server Domain Members** page displays.
3. Click the **Add** button. The **Add Domain Member** page displays.
4. Choose the Conference Server configuration settings. (See below for descriptions of each field.)
5. Click **Submit** at the bottom of the **Add Domain Member** page. A page confirming your edits displays.
6. Click **Members** to get back to the **Domain Members** page.

The new Conference Server displays in the domain members list on the Domain Members page. The new Conference Server receives its configuration from the administrative server. It can communicate with other servers about activity in the domain.

7. Select **Keep List Updated** to update the domain member list automatically every 2 minutes. Otherwise, you have to click the refresh button on your browser to see changes to the list.

Configuration Settings

You can choose the following Conference Server configuration settings:

Conference Server identifiers	Enter the name and IP address of the Conference Server you are adding to the domain. • The name does not have to be a formal host name for the system. It can be a nickname for the system, or any combination of up to 50 characters. • The Conference Server checks for legal IP addresses. A legal IP address is a four-byte quantity written in standard dot notation - for example, 123.45.67.89.
Maximum simultaneous participants allowed	Enter the maximum number of participants that can connect simultaneously to the Conference Server.
Port range to facilitate H.323 data transversal -	Enter the range of port values for transferring H.323 data.
Bandwidth limits per conference -	Enter the maximum send and receive rates for each participant.
Master conference list	Select this option to let this Conference Server host the master conference list.
Historical statistics settings	Enter parameters for how to log statistics for the Conference Server you are adding.
Gatekeeper settings	Choose whether the Conference Server will use an H.323 gatekeeper (either its own or a third-party gatekeeper.) Enter the gatekeeper parameters as applicable.

Once you add a Conference Server to a domain, you can:

- **Add -** Add a new Conference Server to the domain and enter the (server-wide) settings.
- **Edit -** Edit the Conference Server (server-wide) settings.
- **Remove -** Remove the Conference Server from the domain.
- **Shut Down -** Stop the Conference Server and allow automatic restart, or shut it down completely.

Gatekeeper Settings

You can individually configure each Conference Server in a domain for H.323 gatekeeper services. Click the appropriate gatekeeper button and fill in the fields that apply

Optional Gatekeeper terminal aliases for Conference Server

The Conference Server lets you associate a unique identifying string with an H.323 endpoint. The string, called a terminal alias, identifies an endpoint when it registers with the gatekeeper. Certain gatekeepers require that endpoints register using a specific format. The **Optional Gatekeeper terminal aliases for Conference Server** option allows you to customize a terminal alias to conform to gatekeeper requirements.

You can specify the following terminal aliases:

- **H.323-ID terminal alias -** H.323 endpoints generally use H.323-ID terminal aliases to specify which endpoints to connect to through a gatekeeper. An H.323-ID terminal alias can contain any keyboard character up to a maximum of 128 characters.
- **E.164 terminal alias -** H.320 endpoints use E.164 terminal aliases to connect to H.323 endpoints through a gateway or gatekeeper. An E.164 terminal alias can be up to 128 characters in length and contain any digit (0-9), plus the special characters pound (#) and asterisk (*). The hyphen (-) character is not valid for an E.164 address. E.164 terminal aliases are often in the form of a phone number.
- **None –** This is the default setting for the Conference Server gatekeeper functionality. When you select **None**, the Conference Server does not use a gatekeeper for H.323 conferences.

  Select this option if:

  - You do not plan to enable any H.323 conferences on this server.
  - You plan to enable H.323 conferences on the server, but do not plan to have any H.323 clients connecting to those conferences using RAS (Registration, Admission, Status) messaging.

Enter a terminal alias in the **Optional Gatekeeper terminal aliases for Conference Server** field and select **E.164** or **H.323-ID** from the drop-down box. If you need additional fields, click **More**.

If you configure the Conference Server to use a gatekeeper, it automatically registers with that gatekeeper an H.323-ID and an E.164 terminal alias for each of its H.323-enabled conferences. The following fields govern the syntax in creating those aliases:

H.323 Domain Name

This is an optional field, but RADVISION recommends that you complete it.

By default, the Conference Server uses the host name of the computer on which it resides as the suffix for the H.323-ID terminal alias it creates. However, certain gatekeepers require that terminal aliases use a domain name suffix instead. If you enter a domain name, the Conference Server uses it as the suffix for the H.323-ID terminal aliases.

If you have multiple servers using the same H.323 gatekeeper in a domain and you want them to use domain names (rather than host names), you must specify a unique domain name for each server.

Note: Synchronizing the servers in the same domain changes the H.323 terminal alias back to the default alias syntax. This incorporates the host name of the computer as the suffix.

Conference Server E.164 Address Prefix

This is an optional field.

You can enter a numeric prefix for the Conference Server to use when it creates E.164 terminal aliases for its H.323 conferences. The Conference Server adds this prefix to the Conference ID (padded to five digits). If you do not assign a prefix, the Conference Server uses the last two octets of the IP address of the system on which it is installed.

No Gatekeeper

This is the default selection if you chose **None** (default) as the Conference Server gatekeeper setting.

Use the Conference Server Gatekeeper

When you select the **Use Conference Server's Gatekeeper** option, the Conference Server uses its own integrated gatekeeper for H.323 conferences. The Conference Server registers as an endpoint with its local gatekeeper. It creates an alias for each of its H.323 conferences and provides those aliases to the gatekeeper. When an H.323 client that use RAS messaging tries to join a conference, it submits an admission request that includes this alias to the gatekeeper.

For more information on how endpoints specify aliases for H.323 conferences, see **H.323: Selecting a Conference Through a Gatekeeper**.

You can set the following optional parameters when you select the **Use Conference Server Gatekeeper** option:

Ignore discovery requests from the following IP ranges

This option instructs the Conference Server gatekeeper to ignore 'discovery request' messages from certain IP addresses or subnets.

When an endpoint (such as an H.323 client) wants to locate a gatekeeper, it sends out a discovery request to a multicast address. Gatekeepers listen to this multicast address for discovery requests. When a gatekeeper receives a request, it automatically sends back a confirmation message. This provides the endpoint with the information it needs to connect to the gatekeeper.

The Conference Server gatekeeper ignores discovery requests from any IP address or range of IP addresses that you specify. This is useful if, for example, your organization has multiple subnets and you are setting up a Conference Server for just one of them. You can specify each of the subnets you want Conference Server to ignore.

You must list one IP range per line. For more information on specifying IP ranges, see **Using IP addresses and subnet masks**.

Conference Server Endpoint Identifier Suffix

This option lets you specify the suffix that the Conference Server gatekeeper uses when it assigns endpoint IDs.

When an H.323 endpoint registers with a gatekeeper, the gatekeeper assigns it a unique identifier (ID). By default, the format that the Conference Server gatekeeper uses to assign endpoint IDs is as follows: 00001_CUSM, 00002_CUSM, 00003_CUSM and so on.

You can use the **Conference Server Endpoint Identifier Suffix** text field to change the default suffix, CUSM, to a customized suffix for your organization.

Use a Third-Party Gatekeeper

When you select the **Use a Third-Party Gatekeeper** option, you instruct the Conference Server to use a third-party gatekeeper rather than its own local gatekeeper. The Conference Server registers as an endpoint with the third-party gatekeeper you specify. It creates an alias for each of its H.323 conferences and provides those aliases to the gatekeeper. When an H.323 client that use RAS messaging tries to join a conference, it submits an admission request that includes this alias to the gatekeeper. For more information on how endpoints specify aliases for H.323 conferences, see **H.323: Selecting a conference through a gatekeeper**.

In order for the Conference Server to use a third-party gatekeeper, you must provide the following information:

- **Remote Gatekeeper IP -** Specify the location of the third-party gatekeeper. Use the server IP address in standard dot notation.
- **Remote Gatekeeper Port -** The H.323 standard specifies port number 1719 as the standard port for H.323 gatekeepers. You can leave this field empty unless you configured the third-party gatekeeper to listen for RAS messaging on a different UDP port.
- **Remote Gatekeeper ID -** Specify the ID of the third-party gatekeeper.

Removing a Conference Server from the Domain

To remove a Conference Server from the domain:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page displays.
2. Click the **Members**. The **Conference Server Domain Members** page displays.
3. From the selection box, select the domain member that you want to remove.
4. Click the **Remove** button. The **Confirm Conference Server Removal** window displays.
5. Click **Remove**.

This server no longer displays in the list of domain members. It does not participate in domain-wide communications. You can add the server back into the domain at any time through the **Add Domain Member** page.

Note: Removing a Conference Server from the domain does not uninstall it.

Shutting Down the Conference Server

To stop or shut down a Conference Server in the domain:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page appears.
2. Click the **Members**. The **Domain Members** page displays.
3. Select the Conference Server that you want to shut down.
4. Click the **Stop** button. A dialog displays to **Confirm Server Stop**.
    - Click **No** if you want to shut down the Conference Server for a moment and then let it restart automatically. Note: For the Conference Server to restart automatically, you must have to start in with the **cs.continuous** command (for UNIX) or with the service application in **Automatic** mode (for Windows).
    - Click **Yes** if you want to shut down the Conference Server and not allow it to restart automatically.
    - Click **Cancel** if you want to back out of the shut down operation and leave the Conference Server running.

When you shut down the Conference Server, its status changes to **Stopped** on the Domain Members page.

Working with Firewalls

Firewall devices protect your organization’s network. If your organization is behind a firewall, you must release several of the ports the firewall controls in order to allow clients outside the firewall to participate in conferences.

A **port** refers to a specific location within a computer's TCP/IP stack. Programs that communicate over the same network use different port numbers to keep the data that they are sending separate. Think of a participant's IP address as an airport and the ports as gate numbers in the airport. Just as different airlines use different gates, different programs use different ports.

In addition, a single program can use several different ports, each for a different activity. For example, the Conference Server uses a combination of several TCP/IP and UDP ports. In an environment with a firewall, you must allow connectivity on several ports for the Conference Server to function optimally.

Two applications cannot share the same port. For this reason, you cannot run the Conference Server and a client conferencing application, such as CUseeMe Pro or NetMeeting, on the same Windows computer at the same time.

The following tables describe the ports that the Conference Server uses.

Table 1: TCP Ports Used by Conference Server

TCP Port	Use
TCP Port 8080	If you plan to use the Administrator Web pages from a system outside your firewall, you must release the port that your third-party HTTP server uses. The Conference Server uses port 8080 by default but allows you to change this.
TCP Port 1503	This port is for client connections to the T.120 server. ***Note:*** For T.120-only conferences, only this port must be open. For T.120-only *linked* conferences, this port must be open in addition to UDP port 7648.
TCP Port 1720	This port is for H.323 call signaling.
TCP Port 7640	This port is for receiving Telnet configuration commands. If you use Telnet to configure the Conference Server from a system outside your firewall, you must release this port.
TCP Port 7648	This port is for CUseeMe-protocol and old Conference Client connections to the Conference Server.
TCP Port 7650	This port is used for old Conference Client connections, and used between Conference Servers for linking
TCP Port 443	This port is used for Conference Client connections

Table 2: UDP Ports Used by Conference Server

UDP Port	Use
UDP Port 1414	This port is for routing H.323 video streams to third-party streaming applications.
UDP Port 1424	This port is for routing H.323 audio streams to third-party streaming applications.
UDP Port 1812	This is the default port for RADIUS authentication requests. Note that some older RADIUS implementations use port 1645.
UDP Port 1813	This is the default port for RADIUS accounting requests. Note that some older RADIUS implementations use port 1646.
UDP Port 7648	This port is for sending and receiving old Conference Client Videochat streams, and for linking between Conference Servers.

UDP Port	Use
UDP Port 24032	This port is for sending and receiving RTP audio and video streams for the CUseeMe protocol used by old Conference Clients, and for linking between Conference Servers. It is for sending and receiving audio only for clients that support RTP on separate ports.
UDP Port 56800	This port is for sending and receiving RTP video streams for old Conference Clients, and for linking between Conference Servers.
UDP dynamic ports (for audio / video)	Conference Server will dynamically negotiate the UDP ports to use for RTP audio and video based on the range specified by the **media-ports** telnet command. The default range is between 2326 and 65535, but the ports can be specified. The command format is **media-ports [min] [max]**, ▪ The minimum value must be greater than or equal to 2326 ▪ The maximum value must be 100 greater than the minimum, and cannot exceed 65535.

Table 3 below summarizes all TCP and UDP ports in use.

Table 3: Port Summary for different Conferencing Scenarios

	CCLT to CSRV	Old CCLT to CSRV	Linking between CSRV	SIP to CSRV	T.120 to CSRV	Browser to CSRV (Web)	client to CSRV (telnet)	RADIUS	H.323 to CSRV
UDP Ports	dynamic	7648, 24032, 56800	7648, 24032, 56800	dynamic				1812, 1813	1414, 1424, dynamic
TCP Ports	443	7648, 7650	7650	5060	1503	8080	7640		1720

RADVISION is currently working to enable more secure firewall traversal. As a security option, you can set up two Conference Servers – one on either side of the firewall. Configure the firewall device to allow only incoming data from the Conference Server outside the firewall, blocking all other incoming streams. Link the two Conference Servers so that participants on both sides of the firewall can have conferences together. Remote participants connect to the Conference Server *outside* the firewall. Local participants connect to the Conference Server *inside* the firewall.

Note: H.323 clients use a static port number for call connection but also use dynamic port selection. Consult your firewall documentation or contact your firewall vendor to find out whether your firewall supports H.323 traffic.

Enabling E-Mail

When you set up the Conference Server, you must define an SMTP (Simple Mail Transfer Protocol) server. SMTP relay enables users to send email invitations for the conferences they create in the MeetingPlanner applet.

To define the SMTP server:

1. Click the **Network** icon on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network**

page displays.

2. Click **E-mail**. The **Define E-mail Server** page displays.
3. In the **IP Address** field, enter the location of the third-party, outgoing SMTP server. Enter the server IP address in standard dot notation.
4. In the **Port** field, enter the port number that the outgoing SMTP server uses. The default is 25. For more information, refer to the product documentation
5. Click **Submit**. A message displays confirming that the Conference Server saved your settings.

When the MeetingPlanner applet sends out email invitations for a videoconference, participants receive an email message similar to the following:

```
Subject: Video conference invitation

You have been invited to the "Monthly Sales Meeting"
videoconference.

Start Date: November 21, 2004 Start Time: 3:00 PM
Conference ID: 25459 URL:
http://111.222.33.4/scripts/radvision.pub.UserAuthen
tication.class?showLogin=CHECKED&confID=25459
```

The URL connects users to User Authentication Web page, where they can submit an authentication form for the conference.

Note: The Meeting Planner sends email invitations only once, even for scheduled or repeat conferences. The MeetingPlanner sends the email invitation when you create the conference. For more information on the MeetingPlanner applet, see **Using the MeetingPlanner Applet**.

Synchronizing Conference Server Domain Members

The Conference Servers in your domain can fall out of sync with the administrative server and Conference Administrator database. Most often, this happens when you make changes to the conference configuration or user database files for your domain while a domain member is not running. When the domain member restarts, it restarts with the configuration and user access information it had at the time it stopped. It has no access to the changes that you made during the time it was not running.

If you synchronize servers while conferences are running, all clients connected to the server(s) become disconnected.

To synchronize members of your domain with the administrative server:

1. Click **Network** on the Conference Server entry page. You can also click the **Network** icon in the navigation bar. The **Network** page displays.
2. Click **Synchronize**. The **Synchronize Members** page displays.
3. Choose the server you want to synchronize. You can select an individual server or all the servers in the domain.
4. Click **Synchronize**. The Conference Server displays a prompt to confirm that you want to synchronize the server.
5. Click **Yes**. The Conference Server displays a confirmation.

Note: If you have multiple servers in a domain, the Conference Server uses the domain name as the suffix for H323-ID terminal aliases. When you synchronize the servers in the same domain, this changes any non-default H323-ID terminal aliases in use, including the aliases that use a domain name as the suffix. When you synchronize servers, the Conference Server changes the H323-ID terminal aliases to use the default alias syntax, which includes the host name of the computer as the suffix rather than the domain name.

Editing Conference Server Settings

To edit server-wide settings for a Conference Server:

1. On the Conference Server entry page, click **Network**. You can also click **Network** in the main navigation bar. The **Network** page displays.
2. Click **Members**. The **Conference Server Domain Members** page displays.
3. Select the Conference Server that you want to edit.
4. Click **Edit**. The **Edit Domain Member** page displays. The Edit Domain Member page displays the same set of configuration settings as the **Add Domain Member** page. You can edit any or all of the settings. For a detailed description of each of the settings, see **Adding a Conference Server to the Domain**.
5. Click **Submit**. The Conference Server applies your edits and displays a confirmation page.
6. To get back to the Conference Server Domain Members page, click **Members**.

Working with the Conference Administrator database

The following sections provide information on managing the Conference Administrator Database. The database enables you to manage conference information and users.

Defining Your Conference Administrator Database

The Conference Administrator database contains user authentication information for the Conference Server domain. This includes information on:

- End user access to conferences
- End user access to the MeetingPlanner applet
- Administrator and moderator access to the Conference Administrator Web pages

The database lists the member servers in the domain and indicates which of them acts as the administrative server. The database also includes information on which servers host which conferences.

The Conference Administrator database installs as part of a Conference Server full installation. It also installs with a Conference Administrator installation (see the **Conference Server Installation and Upgrade Guide**). Although you can install the Conference Administrator on multiple computers, only a single Conference Administrator database can serve in a domain. All instances of the Conference Administrator Web pages, as well as every Conference Server in a domain, must reference the same Conference Administrator database.

When you install the Conference Server, you specify the location of the Conference Administrator Database for the domain. The **Define Database Server** page allows you to change which Conference Administrator database serves the domain.

Note: Do not confuse the Conference Administrator database with the administrative server for the Conference Server domain. The administrative server is a videoconferencing server that keeps master conference configuration information for all servers in the domain. The Conference Administrator database is part of the Conference Administrator Web pages. The database contains user authentication information. You can install the database on a different computer than your administrative server.

To specify the location of the Conference Administrator Database for your Conference Server domain:

1. Click the **Network** icon on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page displays.
2. Click the **Database** button. The **Define Database Server** page displays.
3. In the **IP Address** field, enter the location of the Conference Administrator database for your Conference Server domain. Use the server IP address in standard dot notation.
4. In the **Port** field, enter the HTTP port for the Web server that runs your Conference Administrator Web pages. Refer to the documentation that came with your third-party HTTP server for port information.
5. Click **Submit**.

Managing Organizations in the Conference Administrator Database

The Conference Server uses organizations to manage groups and the users that belong to them. The administrator adds organization records in the Conference Administrator database and assigns pre-configured templates to those organizations. The administrator then assigns user records to the organizations. Through the MeetingPlanner applet (which the administrator also assigns permission to use), users create conferences based on the templates assigned to their organizations.

The Organizations page displays a list of all organization records that are currently available in the Conference Administrator database. A single default organization listing displays when you access the page for the first time. From the Organizations page, you can add, edit, and remove organization records.

Adding an Organization Record to the Conference Administrator database

To add a new organization record:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Organizations** button. The **Organizations** page displays.
3. Click **Add New**. The **Add Organizations** page displays.
4. In the **Organization Name** field, enter a name for the new organization. This field accepts a maximum of 50 characters.
5. Select a template conference from the **Available Templates** selection box. Conferences that you previously created with this template display in this box.
6. Click **Select**. The template conference you selected moves from Available Templates to the Selected Templates box. Repeat this step until all the templates that you want to assign to the organization display in the Selected Templates box. If you change your mind, you can click **<<Deselect** to move it back.
7. Click **OK**. The Conference Server creates the organization record and displays it on the Organizations page.

Editing an Organization Record in the Conference Administrator database

To edit an existing organization record:

1. From the Organizations page, select the organization record you want to edit.
2. Click **Edit**. The **Edit Organizations** page displays.
3. Edit the record and click **OK**.

The Conference Server edits the organization record and returns to the Organizations page. You can click **Cancel** to return to the Organizations page without editing the record.

Removing an Organization Record from the Conference Administrator database

To remove an existing organization record:

1. From the Organizations page, select the organization you want to remove.
2. Click **Remove Selected**. The Conference Server confirms that you want to remove the organization. Removing the organization record also removes the user records

associated with that organization.

3. Click **Yes** to remove the organization record and return to the Organizations page. Click **No** to cancel and return to the Organization page.

Initializing the Conference Administrator Database

The Conference Server allows you to clear the Conference Administrator database of all user and organization records. Initializing the database leaves only a default administrator account, allowing you to start with a clean user database.

Note: RADVISION strong recommends that you backup the Conference Administrator database before initializing it.

To initialize the Conference Administrator database:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Initialize** button on the User Menu page. The **Initialize User Database** page displays.
3. A prompt displays to confirm that you want to clear the database of all existing user and organization records. Click **Yes** to initialize the file. Click **No** to cancel.

If you initialize the user database, the Conference Server reverts to its default settings (Username: Administrator; Password: changeme). RADVISION recommends that you customize this default administrator record again to maintain security.

Backing up the Conference Administrator Database

The Conference Server allows you to create a backup copy of the user records in your Conference Administrator database. It is a good precautionary measure to create a backup of the database periodically. In the event of database corruption, you can restore the records to the date and time of the last backup. The Conference Server creates the backup file, called **users.db.bak,** in the following subdirectories, depending on your operating system:

Table: Back-up File Subdirectories

Operating System	Subdirectory
Windows 2000	Conference Server 7.X.X/jakarta tomcat/webapps/cs/Data
Sun Solaris	Ctm/solaris_59/tomcat/webapps/cs/Data
Red Hat Linux	ctm/linux_24/tomcat/webapps/cs/Data

To back up the user records in the Conference Administrator database, run the installer in the *maintenance* mode. Running the installer in the maintenance mode is only an option for Windows users. Linux and Solaris users do not have this option. Proceed to the **Repair** page to create a backup.

Note: Performing a backup of the user database file only backs up user records. It does not back up organization records.

Adding User Records to the Conference Administrator Database

To add a user access record to the Conference Administrator database:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Add** button. The **Add User Record** page displays.

3. Enter the information for the user identifier fields.
4. Assign user permissions by clicking the **Administrator, Moderator, Conference Manager**, or **General User** button. If you choose **General User**, you must additionally select a user type (**Normal**, **Admit**, **Deny**, or **Admitted Sender**). For a description of the user permission types, see **Assigning Special Permissions**.
5. If the user that you are adding needs to access the MeetingPlanner applet, select an organization name from the **Organization** menu. You must first define the organization in the **Users: Organizations** area of the Conference Administrator database. When you select an organization, the appropriate templates for that organization display in the **Templates assigned to this organization** box.
6. From the **Conference** menu, select a specific conference, ****All Conferences****, or ****Unassigned****. This selection determines the conference or conferences for which the special permission applies. Note that Administrator permission does not require that you select a conference — by default, it applies to all conferences.

   Note: Selecting ****Unassigned**** means that the Conference Server adds the user record, but does not apply it to a conference. This is handy if you want to add user records in advance of creating the conference. You can go back at any time to edit the record and assign it to a conference.
7. Click **Add User**. The Conference Server adds the new record in the Conference Administrator database.

If you want to assign the same permission to a user for multiple conferences, you must add separate user records for each conference. For example, to assign Moderator permission to User A for Conferences 2 and 4, you must add two user records for User A. The first user record assigns Moderator permission for Conference 2. The second user record assigns Moderator permission for Conference 4.

If you try to submit a user record that has the same Username and Conference as an existing record, the Conference Server considers it a duplicate. You must change the record or cancel the submission.

The **Add User Record** page contains the following user identifier fields:

User Identifier Fields

Username	For user records assigned the **Administrator**, **Moderator**, or **Conference Manager** permission. Username is also required when admitting users to conferences that use **Username/Password** authentication. Username accepts a maximum of 32 characters.
Password	For user records assigned the **Administrator**, **Moderator**, or **Conference Manager** permission. It is also required when admitting users to conferences that use **Username/Password** authentication. Password accepts a maximum of 15 characters. This field is required.
Last Name	For identifying users in the user database. **Last Name** accepts a maximum of 35 characters. This field is optional.
First Name	For identifying users in the user database. **First Name** accepts a maximum of 35 characters. This field is optional.
Email Address	For user records assigned the Conference Manager permission. **Email Address** is a return address for email invitations sent out through the MeetingPlanner applet. Email Address accepts a

	maximum of 50 characters. This field is required.
IP Address -	For user records assigned the **Admit**, **Deny**, or **Admitted Sender** permission under **General User**. **IP Address** accepts a maximum of 15 characters. You can specify an IP address for an individual user or for multiple participants in the same IP subnet. This field is required.

Note: The user identifier fields do not accept the following characters: double-quote ("), single quote ('), back slash (\ ), forward slash (/), semi-colon (;), asterisk (*), question mark (?), and percent sign (%). Additionally, the Username and Password fields do not accept spaces.

Searching User Records in the Conference Administrator Database

The **Search** button on the User Menu page links you to the **Search User Database** page. Once you populate the Conference Administrator database with user records, it is good practice to search the database before adding a new record. You can sometimes edit an existing user record rather than adding a new one. By avoiding redundant user records, you can minimize the size of the user database.

The **Search User Database** page contains the same user identifier fields as the **Add User Record** page, except for the Password field. You can search on any single field or any combination of fields. For example, a search on the last name 'Smith' returns a list of all the user records with that last name. A search on the last name 'Smith' and 'Conference 3' returns a list of all users with the last name 'Smith' that have a user record for Conference 3. The more fields you enter as search criteria, the more narrow the search becomes.

By default, the (General User) **User Type**, **Organization**, and **Conference** selections on the Search User Database page are empty. Unless you specifically select one of them, these fields are not part of your search criteria. The Conference menu also has ****Unassigned**** and ****All Conferences**** search options. When you select ****Unassigned**** as part of your criteria, the Conference Server searches for records that are not associated with any conference. When you select ****All Conferences****, it searches for records that are associated with all conferences in the domain.

To search the database, enter the search criteria in the appropriate field(s) and click **Search**. The **Select User Record** page displays with the results of the search. For example, you can enter search criteria of **First Name** 'Barbara' and **Last Name** 'Smith'. If Barbara Smith is an admitted sender in Conference 0 and a Moderator in Conferences 2 and 5, *three user records* display in the search results.

From the **Select User Record** page, you can also edit, copy, or remove a user record.

Note: The Conference Server can display up to 100 user records on a single page. To see the next page of user records, click **More**.

Editing User Records in the Conference Administrator Database

Once you add a user record to the database, you can make modifications to the record at any time.

To edit a user record:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Search** button. The **Search User Database** page displays.

3. Enter the search criteria and click **Search**. The **Select User Record** page displays with the results.
4. Select the user record you want and click **Edit**. The **Edit User Record** page displays.
5. Enter your edits and click **Submit Edits**. The Conference Server updates the user record with your changes and then displays the Search User Database page.

From the **Edit User Record** page, you can also click **Delete Record** to remove a record from the database.

Copying User Records in the Conference Administrator Database

You can copy an existing user record and use it as a starting point for a new record. This is handy, for example, if you want to assign the same permission to a user for multiple conferences. By copying the record, you do not need to enter the information multiple times - you can edit the portion of the record that is different.

To copy a user record:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Search** button. The **Search User Database** page displays.
3. Enter the search criteria and click **Search**. The **Select User Record** page displays with the results.
4. Select the user record you want and click **Copy**. The **Copy User** page displays.
5. Enter your edits and click **Copy User**. The Conference Server adds a new record with your changes and then displays the Search User Database page.

Note: When you copy a user record, you must at least change the Username or Conference field. If you try to submit a user record that has the same Username and Conference as an existing record, the Conference Server considers it a duplicate. You must change the record or cancel the submission.

Removing User Records from the Conference Administrator Database

To remove a user record from the Conference Administrator database:

1. Click the **Users** icon on the Conference Server entry page. You can also click the **Users** icon in the main navigation bar. The **User Menu** page displays.
2. Click the **Search** button. The **Search User Database** page displays.
3. Enter the search criteria and click **Search**. The **Select User Record** page displays with the results.
4. Select the user record you want and click **Remove Selected**. The **Remove User Record** page displays with a confirmation that you want to remove the selected user record.
5. Click **Yes**. Conference Server removes the user record and then displays the **Search User Database** page.

You can also remove a record from the **Edit User Record** page.

As an alternative to removing user records, you can create an organization for inactive records and move user records to it.

Conference Server T.120 Features

The T.120 security feature is a server-wide feature that is disabled by default. If you enable it, the T.120 server allows you to initiate and accept secure calls only. You can enable this feature manually, or you can use the Telnet T120-encryption command.

Data Conferencing with the Conference Server T.120 Server

The Conference Server is actually two integrated servers with a common user interface. In addition to a videoconferencing server, the Conference Server includes an integrated T.120 server for data conferencing. The Conference Server's T.120 server makes it easy to add multipoint data conferencing to a videoconference. Depending on the T.120 client applications used, participants can share, edit, and annotate documents and images, view formal presentations, and even share applications such as spreadsheet or word processing programs.

The Conference Server's T.120 server provides the benefits of client/server architecture to multipoint data conferencing. These benefits include:

- **Improved performance and reliability for large conference hosting**

  The Conference Server's T.120 server improves the multipoint performance of T.120 client applications. Conference Server's T.120 server handles all multipoint data processing, taking the burden off the computer systems of individual participants and allowing more participants to connect.

- **Reduced network traffic**

  Network managers can reduce network traffic by distributing and connecting multiple Conference Server T.120 servers throughout an organization's wide area network (WAN).

- **Client access control, conference scheduling, and more**

  The Conference Server allows you to set rules for a data conference, which is not possible in a client-controlled conference. With the Conference Server, the parameters you set for any videoconference also apply (where possible) to your data conference. These parameters include user authentication and access, conference scheduling, conference time limits, password, and maximum number of participants allowed.

- **Increased flexibility**

  The Conference Server's T.120 server provides participants the flexibility to come and go from a conference. Without the T.120 server, the originator of the conference would have to stay in the conference.

About T.120 Transport Security

The Conference Server supports a T.120 transport security feature that provides data encryption. Currently, only the Windows platform supports this security feature. You can enable or disable the T.120 transport security on a server-wide basis through the T.120 configuration file, the t120-encryption Telnet command, or through the user interface.

For T.120 transport security, the ITU defined T.123 Annex B, which defines a protocol that allows transport connections for T.120 conferences to negotiate the availability of extended services. These extended services include security protocols, transport protocols, levels of reliability of data transfer, and support for address aliases. T.123 Annex B has provisions for both standard and non-standard security protocols. These

include the following standard security protocols:

- Generic Security Service Application Program Interface (GSS-API),
- Secure Socket Layer Top Level Specification (SSL/TLS)
- X.274
- IPsec (IP Security)

Currently, only NetMeeting 3.0 on the Windows platform supports the Conference Server T.120 security features.

GSS-API and SSL/TLS

The Internet Engineering Task Force (IETF) designed the GSS-API to provide a generic security service, independent of the underlying security and transport mechanism. Applications use GSS-API to generate and process security tokens, but the applications themselves are responsible for the exchange of the security tokens. The security tokens are transparent to applications. In accordance with T.123 Annex B, GSS-API is layered above the X.224 class 0.

Netscape originally developed the SSL security protocol. TLS is an IETF standard that is based on SSL version 3.0. The protocol allows client-server applications to communicate over a stream-oriented transport in a way that prevents eavesdropping, tampering, or message forgery. The protocol also allows optional identity authentication of peers to protect against identity spoofing and unauthorized access.

TLS uses a combination of symmetric key and asymmetric key cryptography. Asymmetric key cryptography authenticates and negotiates the symmetric keys used for encryption and message authenticity. In theory, TLS allows total anonymity; neither client nor server verifies the other's identity. In practice, the client (for instance, the Web browser) usually verifies the server identity.

Digital Certificate

The primary TLS authentication mechanism is the digital certificate, a form of electronic documentation that verifies the identities of parties engaged in online transactions. Digital certificate technology is based on the standards in Recommendation X.509 of the International Telecommunication Union -Telecommunication Standardization Sector (the ITU-T). First, an entity requests a certificate from a Certificate Authority (CA). The CA then decides, using its published criteria, whether to issue the certificate to the entity. If the entity satisfies the CA criteria, the CA issues the certificate and digitally signs and approves it. The certificate binds the entity and the entity's public key to a name called the *unique distinguished name*, or DN. The DN must be unique for each entity certified by the CA, but the CA may issue more than one certificate with the same DN to the same entity.

The T.120 Configuration File

The **T.120 configuration file** is a simple text file containing T.120 server-wide configuration information. You can edit this file with a text editor.

The format of the configuration file is similar to that of the Windows .**INI file**. A configuration entry is defined as a name-value pair. The name-value pairs are in turn grouped into sections. Any line which begins with a **'#'** or **';'** character is treated as a comment.

The following shows the general format of the T.120 configuration file:

```
[<section>]
<name>=<value>
```

- Windows Registry under **HKEY_LOCAL_MACHINE\SOFTWARE\Click to Meet\Conference Server\7.x.x\T120**.
- On UNIX, the environment variable **T120_CONFIG_FILE** is used instead. If the registry key or the environment variable is not set, the T.120 stack assumes that the configuration file is named **T120.cfg** and can be found in the current working directory of **confsrv.exe** process.

  By default, the configuration file is **T120.cfg** and is located in **/usr/local/ctm/confsrv/**.
- On Windows, the install directory is usually **...\Program Files\Click to Meet\Conference Server 7.x.x**
- On Unix, it is typically **/usr/local/ctm/confsrv**.

The following code is an example of a typical T.120 configuration file on Windows:

```
[NCNodeAttributes]
ManagementDevice=0
Peripheral=0
NodeName=Click to Meet Conference Server
7.3.0.12@yallara
SiteInformation=RADVISION T120 Conference Center
[MCSDomain]
minThroughputInterval=15
minSuperiorThroughputInterval=0
[Transport]
Security=0
[CNP]
UseHeader=0
```

Enabling the T.120 Security Feature

You can configure the security feature manually through the T.120 configuration file. The **Security** parameter is in the **Transport** section of the file. The **UseHeader** parameter is in the **CNP** (Connection Negotiation Protocol) section of the file.

To configure T.120 security:

1. Shut down or stop the Conference Server.
2. With a text editor, open the **T120.cfg** file in the Conference Server install directory.
3. Find the Security parameter in the Transport section of the file.

To enable the security feature, enter **1**. To disable it, enter **0**. If the Security parameter is absent from the T.120 configuration file, the security feature is disabled.

The configuration below enables the security feature:

```
[Transport]
Security=1
```

4. Find the **UseHeader** parameter in the **CNP** (Connection Negotiation Protocol) section of the file.

To enable the (CNP) header, enter **1**. To disable it, enter **0**. If the CNP parameter is absent from the T.120 configuration file, the CNP header is used. Although the T.123 Annex B standard requires the use of the CNP header, this parameter must always be set to 0 or disabled in order to use NetMeeting 3.0 effectively.

The configuration below disables the CNP header:

```
[CNP]

UseHeader=0
```

5. Save changes to the **T120.cfg** file.
6. Restart the Conference Server.

Note: As with all other features that you configure through the T.120 configuration file, you must restart the T.120 server before the new setting takes effect.

T.120 Throughput Enforcement

The current T.120 flow control mechanism regulates the data rate in a conference to match the rate of the slowest receiver. This ensures that no two receivers in a conference are too far out of synchronicity. This is important for application sharing in conferences.

One disadvantage of the flow control mechanism is that it is possible for one bad receiver to stop the data flow in the conference. In order to address this issue, the Conference Server uses **T.120 throughput enforcement**.

The Conference Server throughput enforcement works with throughput enforcement *intervals* rather than throughput enforcement *rates*. You define throughput enforcement intervals in seconds – one interval for connections to clients and another for connections to other Conference Servers. You can set both intervals in the T.120 configuration file. The intervals can range from **0** to **600** seconds.

In a typical throughput enforcement scenario, a sluggish client or a subordinate Conference Server stops accepting T.120 data due to network congestion or inadequate bandwidth. When the client stops accepting data, the Conference Server begins timing the interval. When the interval surpasses the limit, the T.120 connection terminates.

When a connection drops due to throughput enforcement, the server's event console or log file displays the following message:

client - T.120 session closed due to insufficient bandwidth

The interval for connections to superior (in the linking topology) Conference Servers must always be greater than the interval for connections to terminals. This encourages throughput enforcement at the lowest possible level in the connection hierarchy, while still disturbing as few nodes as possible. The following rules determine the throughput enforcement interval in various topologies:

- The throughput enforcement interval for a connection between a Conference Server and a terminal is always the value of the **minThroughputInterval** parameter in the configuration file. If the parameter is absent from the configuration file, a default interval of 15 seconds is assumed.
- The throughput enforcement interval for a connection between a subordinate and a superior Conference Server is always the value of the **minSuperiorThroughputInterval** parameter in the configuration file. If the parameter is absent from the configuration file, throughput enforcement is disabled.

Throughput enforcement only occurs in a downward flow from a superior Conference Server to a subordinate one. It never occurs in the opposite direction. In both cases, if the parameter values are out of range, the default values are assumed.

To configure the T.120 throughput enforcement interval:

1. Shut down the Conference Server.
2. With a text editor, open the **T120.cfg** file in the Conference Server install directory
3. Find the following information:

```
[MCSDomain]
minThroughputInterval=
minSuperiorThroughputInterval=
```

To set the throughput enforcement interval, you must change these values. Note that the interval `minThroughputInterval=` takes a value between **0** and **600** seconds. If it is set to **0**, *throughput enforcement is disabled.*

For example, the following will set the interval for all connections to terminals to 30 seconds and for connections to superior MCUs to 5 minutes (300 seconds).

```
[MCSDomain]
minThroughputInterval=30
minSuperiorThroughputInterval=300
```

4. Save changes to the **T120.cfg** file.
5. Restart the Conference Server.

Querying Status of T.120 Security

If you enable the T.120 security feature, all T.120-enabled conferences display an @ character in the attributes on the Conferences page. You can view conference attributes using the telnet **conf** command or the **t120-encryption** command.

The following is an example of the **conf** command output.

```
Conference Server@jking> conf
            1  ACVWEY@ (0/0) test
Conference Server@jking>
```

Joining a T.120 Conference

If you enableT.120 security, NetMeeting requires that you call into the Conference Server using only the T.120 protocol. To call into the Conference Server, use the following NetMeeting **callto** string.

```
Callto:<server ip>+h323=false+secure=true
```

This callto string instructs NetMeeting to initiate a secure T.120 call to the server. The Conference Server displays a dialog box from which you can select the T.120 conference.

Inviting a User into a T.120 Conference

If you enable T.120 security, NetMeeting requires that you use the Telnet **t120-callep**

command instead of the **h323-callep** command to invite a user into a conference. If you use the **h323-callep** command and NetMeeting is configured to accept only secure incoming calls, NetMeeting does not terminate the H.323 call when the user hangs up. Consequently, the corresponding H.323 client object remains in the Conference Server **who** list.

Linking T.120 Servers

The T.120 security settings must be the same (all enabled or all disabled) for servers that you link. Make certain that you make all of the necessary configuration changes to the T.120 configuration file.

The User Authentication Page and T.120

When you enable T.120 security, calls that you make from the User Authentication page are T.120-only calls.

Configuring T.120 Conferences

You set up and control T.120 data conferences in the Conferences area. As a Conference Server administrator, you decide when you set up a conference whether to make data conferencing available to its participants.

Enabling T.120 for H.323 conferences

To enable data conferencing for an H.323 videoconference, select the **H.323 w/T.120** option when you add or edit a conference in the Conferences area. When you submit the conference settings, the Conference Server creates and starts a matching T.120 data conference on its integrated T.120 server. No special configuration of the T.120 conference is required.

If you configure two or more Conference Servers to host the same conference, the Conference Server creates and starts matching T.120 conferences on each server. Furthermore, if you link these Conference Servers together, the T.120 conferences link also.

For example, a corporation with a wide-area network (WAN) has one Conference Server (with an integrated T.120 server) in the corporate office and another in a remote office. For a sales training session, the conference administrator creates an H.323 conference with a matching T.120 conference on the server at each location. The administrator then links the two servers over the WAN in a bi-directional conference. Participants at each location connect to their local servers for bandwidth savings. In effect, the two conferences become one and all participants can videoconference and data conference together.

Note:

- When linking Conference Servers, the conference configurations must be identical on each server. If the configurations are not identical, the T.120 servers do not link properly.
- If you link an H.323 conference between multiple servers, you must designate one T.120 server as “top provider” for the conference. The top provider creates the T.120 conference and then invites linked servers to create their T.120 conferences. You designate a T.120 server as top provider for the conference when you define the Conference Server layout. For more information, see **Working with the Conference Server Layout Applet**.
- If you link a videoconference with a matching T.120 conference between multiple servers, you must create a bi-directional link so that information flows in both directions between the servers. If you create a uni-directional link, audio and video flow in *one direction*

between servers and the T.120 portion of the conference does not link.

- The T.120 portion of a conference does not adhere to observer/observer broadcast rules. This means that users can send T.120 data even if they are not admitted senders for the conference.

Enabling T.120 for non-H.323 conferences

To enable data conferencing for a non-H.323 videoconference, select the **Enable Data Collaboration Server** option when you add or edit the conference in the Conferences area.

Note:

- Only CuseeMe protocol users can connect to a non-H.323 videoconference. However, other T.120-capable clients can connect to the *associated* T.120 data conference. This enables you to create a data-only conference for T.120-capable H.323 client users, or T.120-only users, if you choose.
- The T.120 portion of a conference does not adhere to observer/observer broadcast rules. This means that users can send T.120 data even if they are not admitted senders for the conference.

H.323 and the Conference Server

Hosting H.323 Conferences

As videoconferencing becomes more common, interoperability becomes increasingly important. With users from around the globe communicating with hardware and software from a variety of manufacturers, industry standards are required to ensure interoperability. The Conference Server is a standards-based solution that provides multipoint conferencing services to H.323 standards-based clients. These clients include CU Web, CuseeMe Pro, and the Click to Meet Conference Client.

The H.323 standard serves as the umbrella for a suite of recommendations defined by the International Telecommunication Union (ITU). The H.323 standard defines videoconferencing over packet-switched (generally IP-based) networks such as local area networks (LANs) and the Internet. It covers both point-to-point and multipoint audio and video conferencing. In addition, the ITU defined the T.120 standard to address the document sharing (data conferencing) portion of multimedia conferences.

The Click to Meet Conference Server is a standards-based solution. By connecting to a Conference Server, point-to-point videoconferencing clients that use H.323 standards can participate in multipoint conferences. The Conference Server provides much of the server-based control for H.323-capable clients in the same way that it does for CU Web, CuseeMe Pro, or the Click to Meet Conference Client. These features include security and authentication, client access control, conference administration, and monitoring services for multimedia group interaction.

With the Conference Server, the H.323 standard is a conference attribute (just like audio, video, and chat). When you enable the H.323 attribute in the conference configuration, H.323 clients can connect and participate in the conference. There are, however, some inherent limitations on how H.323 clients can participate in multipoint conferences. This is due, in part, to the fact that engineers designed most H.323 clients for person-to-person videoconferencing rather than group videoconferencing. The Conference Server adjusts for this by performing some special functions behind the scenes.

Receiving video and audio

When you enable the H.323 protocol in a conference, you must also specify the H.323 audio and video codecs. The H.323 standard specifies H.261 and H.263 codecs for video and G.711 and G.723.1 codecs for audio (in addition to others). If you do not specifically choose certain codecs, the Conference Server automatically sets the required audio codec to G.711 (m-Law, 64 Kbps) and the required video codec to H.261 CIF.

Not all H.323-enabled clients support all H.323 audio and video codecs. If an H.323 client connects to an H.323 conference that requires a codec that it does not support, the client can stay in the conference but cannot send or receive the data stream (audio or video) for which it does not have the required codec. For more information, see **Preferred/Required Codecs**.

Note: The G.723.1 codec is also referred to as the G.723 codec.

As previously noted, engineers designed most H.323 clients for person-to-person videoconferencing as opposed to group videoconferencing. As a result, most H.323 users have no standard way within their client applications to choose which participant to view in a conference. However, the Conference Server provides the following ways to control the distribution of video to H.323 clients:

- Default video switching based on audio detection

- H.323 VideoSwitcher Applet
- Continuous Presence Mode option
- Time-based switching

Default video switching

By default, the Conference Server uses audio to determine the video stream that H.323 participants receive. For example, if Participant A is speaking, H.323 participants see the video of Participant A in the remote video window of the client application. The Conference Server also performs audio mixing of H.323 audio streams. If more than one participant speaks at a time, the Conference Server uses an advanced audio algorithm to determine which video stream to send. While the participant is speaking, (s)he sees the video of the person who last spoke, rather than seeing his or her own video. Until another audio/video participant joins the conference, the first (as well as the last) H.323 participant in a conference sees his or her own video reflected back from the server in the remote video window.

You can use the Telnet **set-vswitch-mode** and **set-vswitch-interval** commands to do video switching by interval rather than by audio. For more information, see the **Conference Server Telnet Guide**.

Note: H.323 video switching does not affect CuseeMe protocol participants. CuseeMe protocol users can choose to view up to 12 video windows at a time.

The H.323 VideoSwitcher Applet

Conference Server provides a Java applet that enables H.323 end users to override default video switching for a conference. You can access this applet through a Web browser. The H.323 VideoSwitcher Applet lets you choose which video to view from among multiple participants in a conference, regardless of who is speaking.

The Continuous Presence Mode Option

You can purchase the Continuous Presence Mode option as an add-on. The Continuous Presence Mode option enables H.323 users to receive a remote video stream of up to four conference participants. This is an exciting enhancement for H.323 clients that typically receive only a single remote video stream at a time.

To activate continuous presence for an H.323 conference, choose the H.261-CP4 codec as the required video codec for the conference. The Conference Server merges the video of up to four participants into a single video stream. It divides the continuous presence video stream into four cells, or quadrants. At the start of a conference, the quadrants display the videos of the first four participants to connect. If fewer than four participants connect to the conference, a dark gray box displays in the empty quadrants. If more than four participants connect, the default (audio-based) video switching mechanism determines which videos display in the continuous presence stream.

The Conference Server uses a speaking order first in/first out formula to determine how to replace videos in the stream. If a participant whose video does not currently display in the stream speaks, that participant’s video replaces the video of the participant that displayed for the longest period without speaking. This allows for a natural grace period for each video stream based upon the dynamics of the conference.

If you want to guarantee quadrant placements for specific participants in a conference, you can do so by using the Conference Server Continuous Presence Mode applet. This Java applet enables a Conference Server administrator or conference moderator to "pin" a participant video to a particular quadrant of the continuous presence stream. When a quadrant is pinned, default video switching no longer affects it. For more information, see

Using the Continuous Presence Mode Applet.

Time-based Switching

You can use the Telnet **set-vswitch-mode** and **set-vswitch-interval** commands to do video switching by interval rather than by audio. For more information, see the **Conference Server Telnet Guide**.

Managing Bandwidth with the Conference Server

The Conference Server incorporates considerable intelligence about the nature of real-time rich media communication. It uses this built-in intelligence to route multimedia data streams in the most network-friendly way. As a Conference Server administrator, you can also impose manual limits to further control bandwidth use on your network.

The Conference Server helps you to manage bandwidth with:

- Automatic bandwidth controls
- Manual bandwidth controls
- Multiple server conferences

Automatic Bandwidth Controls

The Conference Server automatically optimizes the use of bandwidth on your network with automatic bandwidth detection and automatic bandwidth pruning.

Automatic Bandwidth Detection

Based on network load, the Conference Server makes adjustments on-the-fly to individual user transmissions. If packet loss starts to reach unacceptable levels because of heavy network traffic, the Conference Server scales back the user transmission rates until network congestion is relieved.

Automatic Bandwidth Pruning

The Conference Server cuts back, or prunes, the amount of data it sends to lower-speed remote participants, instead of flooding them with more data than their connections can handle. This results in considerable network bandwidth savings. The Conference Server does not send data over the network that lower-speed remote participants cannot use. This improves the quality of the conference for all participants. LAN-based participants benefit because their performance is not scaled down to the least common denominator. Remote participants benefit because the Conference Server makes intelligent decisions about what data gets through to them, rather than allowing the network to drop random data packets.

Note: You can get additional bandwidth on a multicast-enabled corporate LAN. The Conference Server builds on the inherent bandwidth savings of IP multicast by bridging multicast and unicast connections. Each remote unicast participant sends a single audio-visual data stream to the Conference Server. The Conference Server then sends (by multicasting) those streams to participants on the corporate LAN. For more information, see **Understanding Unicast and Multicast**.

Manual Bandwidth Controls

As more participants take part in multimedia conferences, it can consume significant amounts of your network bandwidth. In this case, you can put some limits in place. You can manually control how much bandwidth participants use on your network by setting limits by conference or by server:

Setting Conference-Specific Limits

You can control bandwidth by limiting the number of conferences on your network, the number of participants in each conference, and the maximum send and receive rates for each conference. Before setting up a conference, make a rough estimate of the available bandwidth and the anticipated patterns of use. You set conference-specific limits in the Conferences area. You can change the limits you set at any time.

Setting Server-Wide Limits

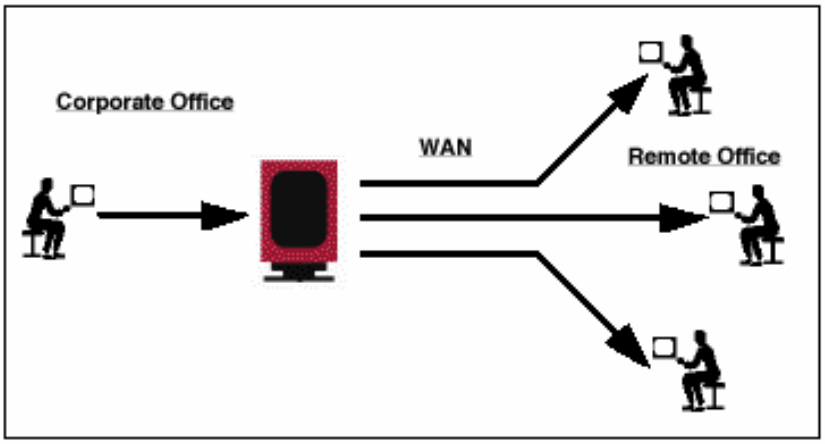
You can also set bandwidth and load control limits on a server-wide basis. If you set server-wide settings that are more restrictive than corresponding conference settings, the server-wide settings prevail. In this way, you preserve the concerns of your network over those of an individual conference. You can set server-wide limits in the Network area when you add or edit a Conference Server to the domain. For more information, see **Bandwidth Controls**.

Setting up Multiple-Server Conferences

You can dramatically increase bandwidth savings by using multiple Conference Servers to distribute the communications load over a wide area network (WAN) or the Internet.

Figure A and Figure B illustrate examples of local replication of conferences. Both figures show a videoconference with four participants – one located at the corporate office and three located in a remote office. For the sake of simplicity, in these examples, communication flows in only one direction.

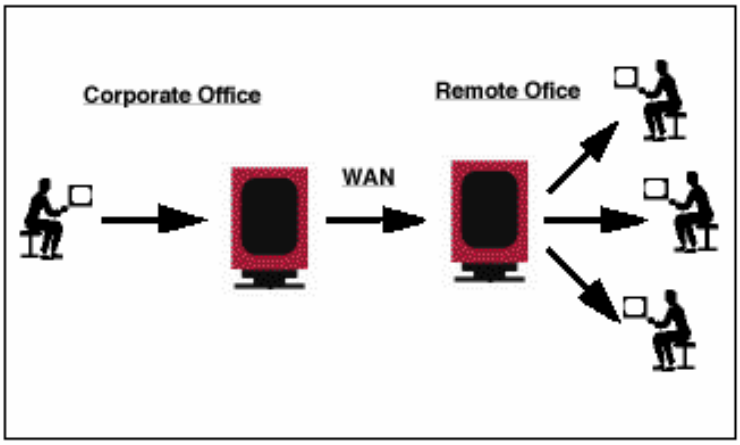
Figure A: Single server conference over Wide Area Network



In Figure A, the conference uses a single Conference Server located at the corporate office. Three copies of the corporate office data go out over the unicast WAN, one copy for each recipient at the remote office.

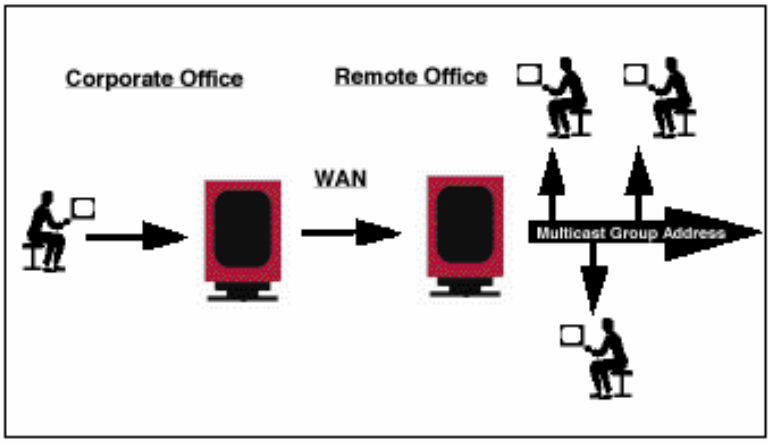
In Figure B, each office has a local Conference Server. The participants connect locally and the Conference Servers communicate with each other across the unicast WAN. A single data stream of the corporate office data goes out over the WAN. The Conference Server then replicates the data stream to each recipient on the remote office local area network (LAN). This saves considerable bandwidth on costly WAN links.

Figure B: Local replication with multiple Conference Servers



Distributing Conference Servers in this way lets you take advantage of the multicasting abilities of your LAN without requiring a multicast WAN or Internet infrastructure as illustrated in Figure C.

Figure C: Local replication with LAN multicast



When you add or edit a conference in the Conferences area, you determine the servers on which it runs. For more information, see **Adding a Conference**.

Participating in Conferences

Selecting a Conference

The Conference Server provides a variety of methods for H.323 client users to choose which videoconference to attend. In addition, CuseeMe protocol users see a list of available conferences when they connect to the Conference Server.

H.323 clients can select a videoconference through:

- An H.323 gatekeeper
- The Conference Server T.120 server
- The User Authentication Web page
- Default H.323 conference routing
- The CallOut applet

Selecting a Conference Through a Gatekeeper

If you configure the Conference Server to use a gatekeeper, it automatically registers two aliases with the gatekeeper for each of its H.323-enabled conferences. H.323 and H.320 endpoints use these two aliases to request admission from the gatekeeper to the conference. The gatekeeper uses address translation to convert the alias addresses to a transport address, enabling the clients to connect.

The Conference Server registers the following aliases for each of its H.323 conferences:

H323-ID Terminal Alias

H.323 endpoints use an H323-ID terminal alias to specify which conference to connect to through the gatekeeper. The Conference Server creates H323-ID terminal aliases using the following syntax:

```
conf<Conference ID padded to 5 digits>@<host name>
```

For example, the default H323-ID terminal alias for Conference 12 hosted on a server with the host name "california" is:

```
conf00012@california
```

You can customize the H323-ID terminal aliases that Conference Server creates. To customize an H323-ID terminal alias, you can do either of the following:

- When you add or edit a domain member in the Network area, specify the domain name where the Conference Server resides. The Conference Server uses that name instead of the server host name to create H323-ID terminal aliases for its conferences.
- When you add or edit a conference in the Conferences area, specify a conference nickname. The conference nickname replaces the portion of the terminal alias that appears before the @ sign. For example, if you choose "training" as the nickname for Conference 12 on host "california", the H323-ID terminal alias is:

  ```
  training@california
  ```

  H.323 users enter this alias to join Conference 12 on the Conference Server.

E.164 Terminal Alias

H.320 endpoints use a numeric E.164 terminal alias to specify which conference to connect to through a gateway/gatekeeper. The Conference Server creates E.164 terminal aliases using the following syntax:

```
<E.164 Numeric Prefix><Conference ID padded to 5 digits>
```

When you add or edit a domain member in the Network area, the Conference Server allows you to specify an E.164 prefix. If you do not specify one, the Conference Server assigns a default E.164 prefix using the last two octets of the IP address of the system on which the Conference Server is located.(An IP address is made up of four groups of numbers in standard dot notation. Each group of numbers represents an 8-bit byte or "octet".) For example, the default E.164 terminal alias for Conference 12 hosted on a system with an IP address of 100.111.222.34 is:

```
22203400012
```

H.320 users enter this alias to connect to Conference 12 on the Conference Server.

Note:

- H.323 users can specify which conference to join using either an H323-ID or E.164 terminal alias. H.320 users can select conferences using an E.164 terminal alias only.
- Users with videoconferencing clients that support Version 2 of the H.323 standard can request that the Conference Server send a conference list in the Q.931 Facility message. This lets them see which conferences are available. In order to request the list, the user must send a destination alias in the following format:

  ```
  <conference list request indicator>@<domain>
  ```

By default, the Conference Server uses ""conferences" as the conference list request indicator and the host name of the computer as the domain. For example, to request a conference list from a server with host name “applegate”, a user sends the following destination alias:

```
conferences@applegate
```

The Telnet gkep-conflist command allows you to customize the text string used as a conference list request indicator. For more information, see the **Conference Server Telnet Guide**.

Selecting a Conference Through the T.120-Based Server

When you enable the H.323 attribute for a videoconference, the Conference Server T.120 server automatically creates a matching T.120 data conference for document sharing. When H.323 clients using the T.120 protocol (for example, with Microsoft NetMeeting V2.1) try to connect to the Conference Server, they first connect to the T.120 server. The T.120 protocol provides a way for these users to choose a specific data conference from multiple data conferences. Once the user connects to a T.120 data conference, the Conference Server automatically connects the user to the corresponding videoconference.

For more information on Conference Server’s T.120 server, see **Data Conferencing with the T.120 server**.

Selecting a Conference Through the User Authentication Web Page

The User Authentication Web page facilitates the routing of H.323 clients. This page is useful for routing H.323 clients into specific conferences without the using the gatekeeper or a T.120 connection. It also authenticates user names and passwords for conferences.

You can instruct H.323 users to connect first to the User Authentication Web page. Users fill out the form on this page and specify the conference to which they want to connect. They also enter the username and password for the conference. When the individual user submits the form, the Conference Server sends a command that associates the user with the conference. When the user connects with a videoconferencing client, the Conference Server automatically routes the client to the specific conference. For more information on the User Authentication Web page, see **User Authentication Web page**.

Selecting a Conference Through Default Conference Routing

When you configure a conference, the Conference Server automatically enables the H.323 attribute. If your Conference Server does not use a gatekeeper, it automatically routes H.323 clients that use RAS messaging into the first H.323-enabled conference available on your server.

Clients that connect using the T.120 protocol (such as Microsoft NetMeeting 2.1 clients) override the default routing by connecting automatically to the T.120 server and then choosing a conference. Other H.323 clients override the default routing by choosing a conference from the User Authentication Web page.

Selecting a Conference Through the CallOut Applet

The Conference Server includes a Java applet that lets users request callouts, or invitations, for potential conference participants. The CallOut applet installs with the Conference Administrator Web pages. Users have access to it through the Web browser.

The Conference Server automatically routes a user that receives a callout into the conference. For more information, see **Using the CallOut Applet**.

Entering a Conference Password

As an optional security feature, the Conference Server lets you apply a password to the conferences you create. A user who tries to connect to a password-protected conference must enter the correct password.

CuseeMe protocol users enter a conference password during the connection process. However, H.323 clients enter a password through the T.120 server, the User Authentication Web page, or the CallOut applet.

When you create an H.323 conference, the Conference Server creates a matching T.120 conference. If you password-protect the H.323 conference, the Conference Server communicates this password to the T.120 server. Any H.323 client that connects using the T.120 protocol (for example, NetMeeting) must first connect to the T.120 server. This initial connection requires that the user enter the password. If the user enters the correct password, the T.120 connection succeeds and the Conference Server admits the user to the corresponding H.323 videoconference. In this way, the Conference Server uses the T.120 server to handle passwords with H.323 clients.

H.323 clients that do not connect using the T.120 protocol (for example, clients that use RAS messaging) can enter a conference password if they use the User Authentication Web page or the CallOut applet. To connect an H.323 user to a password-protected conference through the CallOut applet, you must provide the password for the conference in the applet before issuing the callout. The participant receiving the callout connects to the conference without being required to enter the password. For more information, see **Using the CallOut applet**.

Scheduling

The Conference Server scheduling feature lets you define the following for your conference:

- Start date and time
- Stop date and time
- Duration (in hours)
- Repeat interval (daily, weekly, or monthly)

This is particularly useful if you are not available to start or stop a conference manually. You can also schedule numerous conferences at once without making the conferences available to participants in advance.

The Conference Server has the following scheduling options for new conferences:

- Always enabled
- Always disabled
- Limit access to scheduled time

Always enabled

Always enabled is the default option. With this option, the conference is available to clients as long as the Conference Server is available. Enabled conferences display in the conference list that participants see when they first connect to the Conference Server. If you select this option, **Enabled (E)** displays as an attribute of the conference on the **Conferences** page.

Note: When you create a conference template, you cannot select the **Always enabled** option. You can select it when you create a new conference from an existing template.

Always disabled

Always disabled makes the conference unavailable to clients even if the Conference Server is available. A disabled conference does not display in the conference list that participants see when they first connect to the Conference Server. The conference only displays in the selection box on the Conferences page with the **Enabled (E)** attribute disabled. This indicates that you already configured the conference and that you must enable it for client conferencing by changing the Scheduling option.

Limit access to scheduled time

Limit access to scheduled time restricts the availability of the conference to the schedule you specified. This allows you to configure the conference in advance and to make it inaccessible to clients until five minutes before the start time. When the conference reaches its scheduled stop time, the Conference Server disables it and disconnects any remaining participants.

When you select the **Limit access to scheduled time** option, you must fill in ***all*** of the scheduling parameter fields.

Creating and Configuring Conferences

The following sections provide information on creating and configuring conferences.

The Conferences Area

You can configure all the attributes of a conference from the **Conferences** area of the Conference Administrator Web pages. When you configure a conference, you define the rules for that individual conference.

Before setting up a conference, it is important to have a clear understanding of its requirements. For instance, a small, interactive sales conference with remote participants has different requirements than a CEO's quarterly communication to employees at multiple sites. In turn, a service provider video chat room on extreme sports needs a different setup than a rock concert cybercast.

From the Conferences area, you can:

- Add new conferences
- Edit the existing conferences
- Copy existing conference configurations and modify them to create new conferences
- Create conference templates to use with the MeetingPlanner applet
- Remove existing conferences

You can define basic settings such as conference name, conference ID, conference greeting, maximum participants, and conference attributes. You can choose more advanced options such as multicasting, conference scheduling, and interfacing with third-party billing systems.

Viewing Available Conferences

The top-level page of the **Conferences** area displays a list of conferences for the domain. The Conference Server lists each conference in a selection box with its name, ID number, attributes, and number of connected users. It also displays an icon bar that links to configuration tasks you can perform.

To choose a conference, click the selection box. Click the icons in the task bar to:

- **Edit –** Edit the selected conference configuration.
- **Copy –** Copy the selected configuration in order to create a new conference with the same or similar settings.
- **Remove-** Remove the selected conference from the domain.

If you decide to create a new conference with new settings, click the **Add** icon in the task bar. When you click the **Add** icon, the Conference Server lets you configure a new conference, even if you already selected one.

When you enter the **Conferences** area for the first time, the Conference Server displays a default list of conferences that loaded at installation. The default list is a starting point; you can use these conferences as they are, modify them, or remove them.

The default conferences are on the administrative server. When you add a Conference Server to a domain, the new domain member receives a conference list from the

administrative server. To allow a new domain member server to host a conference, you must edit the Conference Server layout for the conference. The layout defines which Conference Server hosts a conference and what kind of links, if any, exist between the servers.

The conference selection box on the Conferences page gives a snapshot view of the attributes of each conference. A single-letter code above the conference selection box denotes the conference attributes. Enabled attributes display with an asterisk on the line below the letter code. At a glance, you can see the main characteristics of a conference. Below the conference selection box is a Conference Attributes key. Click any conference in the selection box to display its attributes.

Select the **Keep List Updated** option on the Conferences page to update the conference list automatically every two minutes. If you do not select this option, you can click the browser **Refresh** button to see changes.

The following table gives a description of each conference attribute:

Code	Attribute	Description
(A)	Audio	Enables participants to send audio
(B)	Broadcast	Enables one-way broadcast; only admitted senders can transmit
(C)	Chat	Allows participants to send chat
(E)	Enable / Disable	Enables the conference for client access
(H)	H.323 Enabled	Allows H.323 users to participate in the conference and enables a matching T.120 data conference
(I)	Invitation Only	Allows only clients with an invitation to the conference to connect
(K)	Loopback	Allows users to view their own video (CuseeMe protocol self-reflect)
(L)	Local	Keeps participant data streams local to the Conference Server
(M)	Multicast	Enables distribution to clients via multicast group address
(N)	Continuous Presence	Enables continuous presence for the conference
(O)	Broadcast with Participation	Enables two-way interaction between admitted senders and observers; no interaction between observers
(P)	Private	Sets the conference to hidden
(R)	Root	Denotes a master conference; participants are part of all conferences on server
(S)	Self-reflect	Allows CuseeMe protocol participants to view their own video streams in a remote window
(T)	Template	Denotes a conference template, which is not enabled
(U)	Authentication	Denotes that users must authenticate in order to enter the conference
(V)	Video	Allows participants to send video
(W)	White Board	Enables a matching T.120 conference for a non-H.323 conference (CuseeMe protocol participants)

Code	Attribute	Description
(X)	Multicast / Broadcast	Enables multicast
(Y)	Audio Mixing	Allows mixing of several audio streams
($)	SIP Enabled	Enables a conference for a SIP client
(@)	T.120 Encryption	Enables T.120 encryption transport security
(&)	People + Content	Enables dual video streams to see both people and data content
(#)	Encryption	Indicates that a Click to Meet conference is encrypted

Adding a Conference

When you create a conference, you must first define its attributes. Secondly, you must choose the Conference Server to host the conference. Finally, if you choose to link the conference, you set up the linking configuration between servers. The conference that you finally create displays in the conference selection box on the **Conferences** page.

The Conference Server lets you choose H.323 conferences, CUseeMe-protocol-only conferences, and SIP conferences. The type of conference you choose depends on the type of clients that want to connect to it.

A number of videoconference clients on the market today are H.323-compliant. CUseeMe protocol clients that released prior to CUseeMe Pro V4.0 are not H.323-compliant. Generally, RADVISION does not recommend using them in CUseeMe-protocol-only conferences.

CUseeMe Pro V3.1.*x* clients on both the Windows and Macintosh platforms, while not strictly H.323-compliant, can participate in the videoconference portion of an H.323 conference. However, they cannot exchange T.120 data with H.323 clients in the conference. For the most up-to-date information about which endpoints are compatible with the Conference Server, see the RADVISION Click to Meet Web site (http://www.clicktomeet.com).

To create a new conference:

1. Click the **Conferences** icon on the Conference Server entry page. You can also click the **Conferences** button in the main navigation bar. The **Conferences** page displays.
2. Click **Add H.323, Add CUSM,** or **Add SIP**.
3. Enter the conference settings that you want. The **Add H.323 Conference** page, the **Add CUseeMe Conference** page, and the **Add SIP Conference** page are essentially the same, with the exception of a few settings. Each lets you define the parameters for the conference and is divided into basic and optional, advanced settings.
4. Click **Next** at the bottom of the Basic Settings or Optional/Advanced Settings area. The **Define Conference Server Layout** page displays.
5. In the Conference Server layout applet, define the server to host the conference. For specific instructions on using the applet, see **Defining a Server Layout for Your Conference**.
6. Click **Apply** in the layout applet toolbar. An applet window displays prompting you to save the conference.
7. Click **OK**. The Conference Server displays a confirmation page.

If you want to cancel the conference creation, click the **Cancel** button rather than the **Back** button in the browser.

Basic Settings

You can choose the following basic settings:

Setting	Description
Conference ID	Enter the conference ID that you want to use.
Conference name	Enter the name of the conference.
Private	Select this option to hide the conference. Clear this option to display the conference when users first log in.
Conference greeting	Enter a greeting to display to participants when they first join the conference.
Conference attributes (Video, Audio, Chat, H.323 w/T.120, and SIP)	Select the attributes for this conference. You can choose: • Video • Audio • H.323 with T.120 (displays on the Add H.323 Conference page only) • SIP • People & Content (displays on the Add H.323 Conference page only)
Broadcast mode	Select the type of conference broadcast you want. You can choose: • Normal • Broadcast • Allow audience to interact with sender
Maximum participants	Enter the maximum number of participants for the conference.
Message	Enter the message that you want to display to people who try to connect after the conference reaches the maximum number of participants.

Conference ID

Conference ID is a number used to identify a conference. It display with the **Conference Name**. Enter a number **between 0 and 65,525**.

Each conference must have a unique ID. The Conference Server displays an error if you try to create a conference with an ID number that is already in use in the domain.

Private

The **Private** attribute keeps the conference from being displayed in the conference list. This adds an additional measure of security.

To connect to a private conference, users must know the Conference ID. CUseeMe protocol users can enter this information in the connection dialog. H.323 users can specify a Conference ID when they connect through the User Authentication Web page or use a terminal alias when connecting through a gatekeeper. NetMeeting users can also specify the

Conference ID, followed by a space and the Conference Name in the Advanced calling dialog box of their client application.

Conference Name

The **Conference Name** describes the conference and displays with the **Conference ID** in the conference selection box and on the **Conferences** page. You can enter any combination of letters (a - z, upper or lower case), numbers, and spaces, up to 50 characters.

Conference Greeting

The **Conference Greeting** is a conference-specific message that displays when CUseeMe protocol participants first connect. Enter a message of up to 1055 characters (minus the version string that the Conference Server automatically generates, which is approximately 45 characters).

A typical greeting includes the following:

- Name of your organization
- Location of the Conference Server
- Contact information such as an e-mail address and World Wide Web address
- Maximum data transmission rates
- Information about upcoming events

Conference Attributes

You can turn media attributes for your conference on and off individually. To enable or disable any conference attribute, select or clear it under **Conference Attributes**.

You can choose the following media options:

Video (default = on)

When you select the **Video** option, the Conference Server distributes video data between conference participants. If you clear the video option, the Conference Server discards any video that clients send to the conference. Connected clients then display in the Participant List as “lurkers”. A lurker is a client that does not send video.

Audio (default = on)

When you select the **Audio** option, the Conference Server distributes audio data between conference participants. If you clear the audio option, the Conference Server discards audio that clients send to the conference.

Chat (default = on)

This option is available only on the Add CUSM Conference page. When you select the **Chat** option, the Conference Server distributes chat data between CUseeMe protocol participants in your conference. If you clear this option, the Conference Server discards chat that clients send to the conference.

H.323 w/T.120 (default = off)

This option is available only on the Add H.323 Conference page. When you select the **H.323 w/T.120** option, the Conference Server allows H.323 clients to participate in your conference. It also creates and enables a matching T.120 data conference on the

T.120 server (if installed). The matching T.120 conference lets H.323 clients take advantage of server-based data conferencing (H.323 clients must be T.120-capable). For more information, see **Hosting H.323 Conferences** and **Data Conferencing with the T.120 Server**.

SIP (default = off)

This option is available only on the **Add H.323 Conference page**. When you select the **SIP** option, the Conference Server allows Microsoft Windows XP SIP clients to participate in the conference.

People and Content

This option is available only on the **Add H.323 Conference page**. When you select the People & Content option, the Conference Server lets you use the **People & Content** feature in the PictureTel 900 Series endpoints. The term “people and content” refers to an endpoint that has two outgoing video streams; “people” refers to the camera that shows the person in the conference and “content” refers to the laptop computer or any other video source that displays the data content. When you select **People & Content**, you must choose **H.263+** as the video codec.

Note: The Conference Server processes video, audio, and chat from admitted senders even when you clear the respective **Video**, **Audio,** and **Chat** options in the conference configuration.

Broadcast Mode

The **Broadcast Mode** you select for your conference determines how the Conference Server distributes video, audio, and chat data. To select a Broadcast Mode, click either **Normal** or **Broadcast** on the Add Conference page.

Normal

The **Normal** mode creates a two-way interactive conference that distributes video, audio, and chat between all participants.

Broadcast

The **Broadcast** mode creates a conference that distributes data only from admitted senders. While other participants can connect, the Conference Server does not distribute any of their data. Participants who are not admitted senders are observers. Observers cannot send video, audio, or chat. They do not display in the Participants List. If a conference has no admitted senders, it appears empty to the observer even if there are others connected.

The Broadcast mode is useful for cybercast events that have no need for two-way interaction. It eliminates the traffic associated with connected participants, freeing up bandwidth for the one-way transmission of content. This improves the quality of the broadcast, especially for participants on low-speed connections.

You can create a variation on this mode by selecting Broadcast *and* selecting the **Allow audience to interact with sender** option. When you select both of these options, admitted senders can see and interact with connected observers. The observers can see and interact only with admitted senders. This can be extremely useful for lectures or other presentations in which the presenter (the admitted sender) takes questions from the audience (the observers), but does not want the observers to interact with each other. You can further enhance this mode by assigning Moderator status to the presenter in the Conference Server user database.

Choosing the Broadcast mode produces different results than disabling the video, audio, and chat attributes. When you disable the video, audio, and chat attributes, participants display in the Participants List as lurkers. This does not eliminate the traffic associated with the Participants List.

Maximum Participants

You can enter the maximum number of participants you want to allow in the conference. For better performance in interactive conferences, RADVISION recommends breaking down conferences to 10 participants or less. This is because each participant receives some traffic for every other participant in the conference. For participants connecting in low-bandwidth environments, this overhead can become significant.

Once the conference reaches the maximum number of participants, the Conference Server refuses subsequent users that try to connect. CUseeMe protocol users additionally receive a refusal message that you enter in the text field labeled **Message**. The refusal message is limited to 255 characters. You may want to direct CUseeMe protocol users to connect to an alternate Conference Server.

```
This conference is full. Try connecting to Conference 1 on
conference.conferenceserver.com.
```

The maximum number of participants for a conference can exceed the licensed maximum for the individual Conference Server. This is because a conference can be simultaneously hosted on multiple servers. However, each server allows no more than the maximum number of participants (up to its licensed maximum) defined in its server-wide settings.

Optional/Advanced Settings

You can choose the following advanced configuration settings:

- Template Conference
- Conference owner information
- Conference Password
- Scheduling
- Bandwidth controls
- Time limits
- Preferred/required codecs
- Data collaboration server
- User authentication
- Audio latency
- Conference aliases
- Multicast
- Self-reflect
- Root
- Tracking
- Streaming

The following section indicates when a setting is specific to the Add H.323 conference page

or the Add CUseeMe conference page.

Template Conference

The **Template** option lets you use a conference as a template for other conferences. Creating a template allows users to create conferences with the MeetingPlanner applet using the attributes and server layout that you define. You can also define frequently used configurations as templates, copying them to create new templates and conferences.

Template conferences must belong to an organization. If you do not create an organization for a template *before* creating the template itself, it does not display in the list of available templates.

Users cannot connect to a template conference. When you enable the template attribute, the Conference Server automatically disables the conference for users. You can enter text (up to 1000 characters) in the Template Description box that describes the parameters of the template. This text displays in the MeetingPlanner applet and helps users decide which template to choose for a conference.

When you create a template conference, select **Limit access to scheduled time** and enter a value in the **Duration** field. This limits the length of conferences that users can create with the MeetingPlanner applet.

Conference Owner Information

The **Information** option lets you provide conference owner information for multicast session announcements. If you are not using multicast, you can leave these fields blank.

RADVISION implements multicasting according to the standards determined by the Internet Engineering Task Force (IETF). An important part of the standard involves announcing the creation of multicast conferences (also known as multicast sessions). Session announcements serve two purposes:

- They convey ownership and contact information so that interested parties can inquire about participation in the conference.
- They reserve multicast addresses so that other groups planning multicast conferences do not attempt to use the same addresses.

When a conference uses IP Multicast, the Conference Server periodically broadcasts a session announcement on the Internet. The session announcement contains the information you enter in the following fields. If you leave any of the fields blank, they display as empty in the session announcement.

Conference Owner

Provides the name of the conference owner or contact person. This information can be a login name or any other meaningful collection of characters.

E-mail Address

Provides an e-mail address for the contact person or conference owner.

Phone Number

Provides a phone number to call for more information.

Conference URL

Provides the URL or a Web site to visit for more information.

Description

Provides a short descriptive message (limited to 255 characters).

Note: At the time of publication, H.323 clients could not participate in IP Multicast conferences.

Conference Password

To define a password for your conference, enter any combination of characters and spaces in the text field labeled **Password**. A **Password** is an optional security feature that you can apply to your conferences. The **Invalid Password Message** field lets you enter a message that displays to CUseeMe protocol participants if they attempt to connect with an incorrect password. The Conference Server limits the conference Password field to 31 characters and the Invalid Password Message to 255 characters.

H.323 client users can only connect to a password-protected conference through the T.120 server, the User Authentication Web page, or the CallOut applet. For more information, see **H.323: Entering a Conference Password**.

Scheduling

The following sections provide information for configuring conference schedule information.

Start Date

The **Start Date** field is the date that the Conference Server enables a scheduled conference. Scheduled conferences remain disabled until five minutes before the date and time in the Start Date and Start Time fields. You can enter the start date string in the MM-DD-YY format.

A scheduled conference requires that you select the **Limit access to scheduled time** option. You must also enter the Start Date, Start Time, Duration, and Repeat Conference fields.

Start Time

The **Start Time** field is the time that the Conference Server enables a scheduled conference. Scheduled conferences remain disabled until five minutes before the date and time specified in the Start Date and Start Time fields.

You can enter the start time string in the HH:MM format, in the local time of the system to which your browser is connected. The Conference Server converts the local time and starts the conference at the correct time – even if the conference is on multiple servers in several different time zones.

A scheduled conference requires that you select the **Limit access to scheduled time** option. You must also complete the Start Date, Start Time, Duration, and Repeat Conference fields.

Duration

The **Duration** field defines how long a scheduled conference lasts. You specify the duration in hours and minutes, using the HH:MM format (with a maximum of 24:00). When a conference exceeds the duration time, the Conference Server automatically disables it and disconnects any participants with the following message:

```
Conference is terminating.
```

A scheduled conference requires that you select the **Limit access to scheduled time** option. You must also complete the Start Date, Start Time, Duration, and Repeat Conference fields.

Repeat conference

The **Repeat Conference** field indicates whether the Conference Server automatically repeats a scheduled conference daily, weekly, monthly. If you select **Never**, the Conference Server deletes the conference when it is over.

The monthly repeat option schedules a conference on the same day of a particular week in subsequent months. For example, if you specify September 7, 2004 (the first Tuesday of September) as the start date of a conference with a monthly repeat option, the Conference Server schedules subsequent conferences on October 5, 2004 (the first Tuesday of October), and November 2, 2004 (the first Tuesday of November).

If you specify a day during the fifth week of a month as the start date, the Conference Server schedules the conference on that day in the last week of subsequent months. For example, if the start date is June 30, 2004 (the fifth Wednesday of June), the Conference Server schedules subsequent conferences on July 28, 2004 (the fourth and last Wednesday of July), August 25, 2004 (the fourth and last Wednesday of August), and September 29, 2004 (the fifth and last Wednesday of August).

A scheduled conference requires that you select the **Limit access to scheduled time** option. You must also complete the Start Date, Start Time, Duration, and Repeat Conference fields.

Bandwidth Controls

The Conference Server has several manual load controls that help you to manage the load on your servers and your network. In CUseeMe-protocol-only conferences, you can choose the bandwidth controls.

Maximum Send Rate

This option is available only on the Add CUseeMe Conference page.

The Maximum Send Rate field defines the upper limit (in Kbps) to which CUseeMe protocol users can set their send (transmission) rate when connecting to your conference. This allows a participant to connect to a conference only if that setting is *below* the Maximum Send Rate you specified for the conference.

Maximum Receive Rate

This option is available only on the Add CUseeMe Conference page.

The Maximum Receive Rate field defines the upper limit (in Kbps) to which CUseeMe protocol users can set their receive rate when connecting to your conference. If you set the client Maximum Receive Rate to a number higher than the Conference Server allows, the Conference Server automatically negotiates the settings to match for CUseeMe Client version 3.0 or later. The Conference Server denies access to CUseeMe Clients with version 3.0 and earlier.

Time Limits

This option is available only on the Add CUseeMe Conference page.

Setting a time limit lets you define the amount of time that participants spend connected to a conference. In an H.323-protocol-only conference, you can also choose bandwidth

controls.

Bandwidth

This option is available only on the Add H.323 Conference page.

H.323 clients use a single bandwidth setting that combines both send and receive rates.

The Bandwidth section lets you define:

- The **upper limit** (in Kbps) for sending audio and video data

  Note: H.323 endpoints are typically configured using the total of the send and receive bandwidth that in a session. For example, if the configuration of an H.323 endpoint is 768 Kbps, set this field to 384.

- Whether or not to use **Continuous Presence** mode (the default is OFF)

  Note: When you select Continuous Presence, it sets the video codec to H.261. The format for sending video is QCIF, while the format for receiving video is CIF.

- The **frames per second** (fps) for video

Required Codecs

This option is available only on the Add H.323 Conference page.

The Required Codecs option lets you define:

- Audio codec
- Video codec
- Video resolution

When creating an H.323 conference, you must choose one required audio codec and one required video codec. You cannot choose multiple codecs for each category. If you do not choose these options, the Conference Server uses of G.711 (μ-Law, 64 Kbps) and H261.CIF as the default required audio and video codecs.

Each of the H.323 video codecs has a character string that appends its name to the conference, indicating video resolution. The video resolutions are:

- **CIF -** Common Intermediate Format (352 x 288 pixels)
- **QCIF -** Quarter Common Intermediate Format (176 x 144 pixels)
- **SQCIF -** Sub-Quarter Common Intermediate Format (128 x 96 pixels)
- **CP4 -** Continuous Presence (CIF video window divided into four QCIF cells)

The selections for Bandwidth and Required Codecs affect each other. Once you select the overall conference bandwidth, the Conference Server applies restrictions on the amount of transmitted audio and video data. When Continuous Presence is ON, it also adds bandwidth requirements to the conference bandwidth.

The following tables list videoconferencing clients that are compatible with the listed codecs. They are not inclusive of all clients that can connect to H.323 conferences on the Conference Server.

Table: Audio Codecs Available

Audio Codec	For Use with Client

G.711 (μ-Law, 64 Kbps)	CUseeMe Client, H.323, SIP
G.711 (a-Law, 64 Kbps)	CUseeMe Client, H.323, SIP
G.722 (64 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (32 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (24 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (16 Kbps)	CUseeMe Client, H.323, SIP
G.723.1 (6.4 Kbps)	CUseeMe Client, H.323, SIP
G.723.1 (5.3 Kbps)	CUseeMe Client, H.323, SIP
G.729A (8 Kbps)	CUseeMe Client, H.323, SIP
iLBC (13.3 Kbps)	CUseeMe Client, SIP

Table: Video Codecs Available for H.323 Conferences

Video Codec	**For Use With Clients**
H263.QCIF (Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H263.CIF (Common Interface Format)	CUseeMe Client, H.323, SIP
H263.SQCIF (Sub-Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H261.CIF (Common Interface Format)	CUseeMe Client, H.323, SIP
H261.QCIF (Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H261.CP4 Continuous Presence	CUseeMe Client, H.323, SIP **Note:** In order for any endpoint to participate in a continuous-presence conference, the client must negotiate and open different *send* **(QCIF)** and *receive* **(CIF)** video channels. If the client is coming through a gateway, it displays only switched video. If you purchased the Continuous Presence Mode option and entered the option serial number during installation, you can select and enable the H261.CP4 video codec. If you did not purchase the Continuous Presence Mode option, the Conference Server ignores the selection and reverts to the H.261.CIF default video codec
H.264 H.264 Level 1 to 5.1 see H.264 Level description table	CUseeMe Client, H.323, SIP
RTVIDEO	Microsoft Office Communicator

Table: H.264 Level description

Level	Max Video Bitrate (kbps)	Max Format
1	64	QCIF
1.1	192	CIF
1.2	384	CIF
1.3	768	CIF
2	2 000	CIF
2.1	4 000	CIF
2.2	4 000	4CIF
3	10 000	4CIF
3.1	14 000	720p HD
3.2	20 000	720p HD
4	20 000	1080p HD
4.1	50 000	1080p HD
4.2	50 000	1080p HD
5	135 000	1080p HD
5.1	240 000	1080p HD

The Add Conference page displays different options, depending on the conference bandwidth setting you chose.The following table lists the combinations of values Conference Server uses.

Table: Settings for H.323 Conferences

Conference Bandwidth	Frames per Second	Continuous Presence	Audio Codec	Video Codec	Video Resolution
64	5	off	G.723.1	H.263	QCIF
128	10	off	G.723.1	H.263	QCIF
256	15	off	G.711µ	H.261	CIF
384	30	off	G.711µ	H.261	CIF
512	30	off	G.711µ	H.261	CIF
768	30	off	G.711µ	H.261	CIF
1024	30	off	G.711µ	H.261	CIF

The **Defaults** button sets the audio codec, video codec, frames per second, and video resolution to RADVISION' recommendations for the conference bandwidth that you chose. Using the Defaults button always disables the Continuous Presence option.

Time Limits

The **Time Limits** option lets you limit the amount of time participants spend connected to a conference. This is useful if you have a busy Conference Server and want to allow as many participants as possible to have access to it.

You can set the following limits:

Disconnect participants after

The amount of time (in minutes) that participants can remain connected to a conference. The default is 0, indicating no time limit for the conference.

Time limit disconnect time

The amount of time (in minutes) before participants can reconnect to a conference from which they were disconnected (after reaching the time limit).

Restrict Participant Message

The message that the Conference Server displays to CUseeMe protocol participants. This message indicates that the participant reached the conference time limit and can re-connect after the specified disconnect period. (*x* = time limit disconnect time):

For example:

```
Your allotted time in the conference has expired. You may
connect again in x minutes.
```

Data Collaboration for Non-H.323 Conferences

This option is available only on the Add CUseeMe Conference page.

Select the **Enable Data Collaboration server** option to create and start a matching T.120 data conference for a non-H.323 videoconference. The T.120 data conference provides server-based document sharing for CUseeMe protocol participants (version 3.0 or later) in a CUseeMe-protocol-only videoconference.

You can also use the **Enable Data Collaboration server** option to create a data-only conference for H.323-protocol clients that connect with the T.120 protocol.

User Authentication

The following section provides information on user authentication.

Conference Server Authentication

If you select the **Conference Server** authentication option, users must be authenticated through the Conference Server user database before they can connect to the conference. You can choose **IP-based** and **Username/Password** authentication..

IP-Based Authentication

With IP-based authentication, users connect directly with their client conferencing application to your conference. No user can connect to the conference without a user record in the Conference Administrator database. The user record must specify the user's

IP address and assign **General User/Admit** permission for the conference (see **Assigning Special Permission**). The Conference Server checks that the user's IP address is on the admit list for that conference.

While this process is transparent to the user, it does require that the user have a static IP address. You must enter the static IP address in the user's database record for the conference along with the admit permission.

Username/Password Authentication

With Username/Password authentication, users connect to the User Authentication Web page with a browser before connecting to the conference with an endpoint or conferencing application. This allows you to authenticate users through the user database without requiring an IP address.

With username and password authentication, you create one or more user records for the conference in the user database file. You also create an individual user record for each participant, assigning each a unique username and password for the conference with **General User/Normal** permission.

Alternatively, you can create a single record for the entire conference with a group username and password (with General User/ Normal permission) that all participants can use. In either case, you do not need to enter an IP address. From the **User Authentication Web page**, a user can submit an authentication request, specifying username, password, and conference ID. When the user submits the request, the Conference Server receives the authentication query. If authentication succeeds, it issues the appropriate commands and lets the user connect to the conference.

When you use the Username/Password authentication method, you do not need to assign Admit permission in the user record. The Conference Server issues a one-time admit privilege for the user through the User Authentication Web page.

RADIUS authentication

Select the **RADIUS** (Remote Authentication Dial-In User Service) option to enable the Conference Server's integrated RADIUS client to communicate with your third-party RADIUS server. Together, the client and server authenticate conference participants. The Conference Server collaborates with your RADIUS server (rather than its own database) for user authentication information.

If you want the Conference Server to send user connection statistics (or session data) to your RADIUS server for billing purposes, select the **Enable RADIUS accounting** option. In order to enable RADIUS authentication and billing, you must first define the parameters for your third-party RADIUS server in the Network area.

Audio / Video Codecs

You can specify the audio and video codec(s) (COmpression/DECompression algorithms) that clients use in a conference. Clients will use codecs from the specified list. If none of the codecs of a given media type is supported by a client, that client will not be able to send/receive this media.

Audio Codecs

Select the codecs you want to designate Conference page.

Table: Audio Codecs Available

Audio Codec	For Use With Client
G.711 (μ-Law, 64 Kbps)	CUseeMe Client, H.323, SIP
G.711 (a-Law, 64 Kbps)	CUseeMe Client, H.323, SIP
G.722 (64 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (32 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (24 Kbps)	CUseeMe Client, H.323, SIP
G.722.1 (16 Kbps)	CUseeMe Client, H.323, SIP
G.723.1 (6.4 Kbps)	CUseeMe Client, H.323, SIP
G.723.1 (5.3 Kbps)	CUseeMe Client, H.323, SIP
G.729A (8 Kbps)	CUseeMe Client, H.323, SIP
iLBC (13.3 Kbps)	CUseeMe Client, SIP

Video Codecs

Select the video codecs you want to designate on the Conference page. If you are choosing an H.263 annex, enter the annex value. If you enter more than one annex, separate them with a space.

Table: Video Codecs Available

Video Codec	For Use With Clients
H263 QCIF (Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H263 CIF (Common Interface Format)	CUseeMe Client, H.323, SIP
H263 SQCIF (Sub-Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H261 CIF (Common Interface Format)	CUseeMe Client, H.323, SIP
H261 QCIF (Quarter Common Interface Format)	CUseeMe Client, H.323, SIP
H263+ annex F (Advanced Prediction Mode)	CUseeMe Client, H.323, SIP
H263+ annex P.5 (Factor-of-4-Resampling)	CUseeMe Client, H.323, SIP
H.264 Level 1 to 5.1 see H.264 Level description table	CUseeMe Client, H.323, SIP
RTVIDEO	Microsoft Office Communicator

Table: H.264 Level description

Level	Max Video Bitrate (kbps)	Max Format

1	64	QCIF
1.1	192	CIF
1.2	384	CIF
1.3	768	CIF
2	2 000	CIF
2.1	4 000	CIF
2.2	4 000	4CIF
3	10 000	4CIF
3.1	14 000	720p HD
3.2	20 000	720p HD
4	20 000	1080p HD
4.1	50 000	1080p HD
4.2	50 000	1080p HD
5	135 000	1080p HD
5.1	240 000	1080p HD

Audio Latency

This option is available only on the Add H.323 Conference page.

Audio latency is the delay between the time a participant speaks and the time that other clients in the conference hear the same audio. Network devices, the Conference Server, and the sending and receiving client endpoints introduce audio latency all along the call path.

The Conference Server does not always receive audio packets in a continuous stream. “Audio jitter” is the term for variation in the arrival time of audio packets. Before mixing the audio it receives in an H.323 conference, the Conference Server builds in a certain amount of latency in the form of stored audio frames. By storing audio frames, the Conference Server maintains a continuous stream to receiving clients. Without enough latency, receiving clients experience gaps in the audio. With too much latency, audio becomes out of sync with the video.

The Conference Administrator Web pages provide audio latency settings optimized for LAN, WAN, and Internet environments: In a mixed environment where clients are connecting to a conference over different kinds of networks, it is preferable to set the latency value to suit the clients with the better connection. The Conference Server increases the amount of latency as necessary to accommodate jitter from clients with lesser connections.

To specify an audio latency setting for your H.323 conference, select **LAN**, **WAN**, or **Modem** in the **Latency Setting** section of the Add Conference page..

Conference Aliases

This option is available only on the Add H.323 Conference page.

If you configure the Conference Server to use an H.323 gatekeeper, you can specify a **conference nickname** or a **user defined** alias.

Conference Nicknames

When you create a nickname for an H.323 conference, the Conference Server uses the nickname as the prefix for the H323-ID terminal alias it creates for the conference.

The Conference Server registers an H323-ID alias and an E.164 alias with the gatekeeper for each of its conferences. Users reference the H323-ID alias when they connect their H.323 clients to the Conference Server through the gatekeeper.

If you do not assign a conference nickname, the Conference Server uses "confXXXXX" as the default prefix for the H323-ID alias, where "XXXXX" is the conference number padded to 5 digits, leading with zeroes. For example, the default for conference 2 would be "conf00002" See H.323: Selecting a conference through a gatekeeper for more information.

To specify a conference nickname, enter a string of 10 characters or less in the **Conference Nickname** field under Gatekeeper.

User-Defined Aliases

When you create a user-defined alias for an H.323 conference, the Conference Server use the nickname as the alias for the H323-ID terminal alias it creates for the conference.

To specify a user defined conference alias:

1. In the Conference Aliases section, click **Add** under the User Defined heading. A window displays prompting you to **Enter new gatekeeper alias**.
2. Enter the new gatekeeper alias.
3. Select the preferred alias type. You can select **E164 (phone)** and enter a phone number or **H323ID (text)** and enter the H323 ID text in the **Alias** field.
4. Click **OK**. The Conference Server adds the new alias.

To remove an alias, highlight it and click **Remove**. The Conference Server deletes the alias.

Unicast and Multicast

The term *unicast* signifies a point-to-point connection where data is sent from one sender to one receiver over an IP network. The Conference Server expands on the unicast principle, allowing multiple clients to conference together. Each client makes a unicast (point-to-point) connection to a Conference Server, sending a data stream that can consist of audio, video, text, and T.120. The Conference Server receives the data streams and distributes one separate copy to every client in the conference who requests it.

By contrast, in a multicast environment, the Conference Server receives the data streams and sends one copy of each participant’s data stream to a multicast group address. Participants connect to the multicast group address and receive the data from there. IP Multicast is an extension of the IP networking standard, which addresses the need to handle group communications. The Conference Server uses IP Multicast to distribute data streams more efficiently to multiple conference participants.

For example, to send an identical message to everyone in your company, you could write a memo, photocopy it, and put a copy into each employee’s mailbox. This is unicasting — sending a separate copy of the same information to each person. You could accomplish the same task more efficiently by printing a single copy of the memo and posting it in a place where everyone in the office is sure to see it. This is multicasting — sending a single copy of information to a group address. The multicast group address is the electronic equivalent of the office bulletin board.

Figure A shows the Conference Server distributing a single participant's data stream to three recipients in a unicast environment (for simplicity of illustration, we have shown communications flowing in one direction only). Notice Conference Server must send the data stream three times: once for each recipient.

Figure A: Unicast Conference

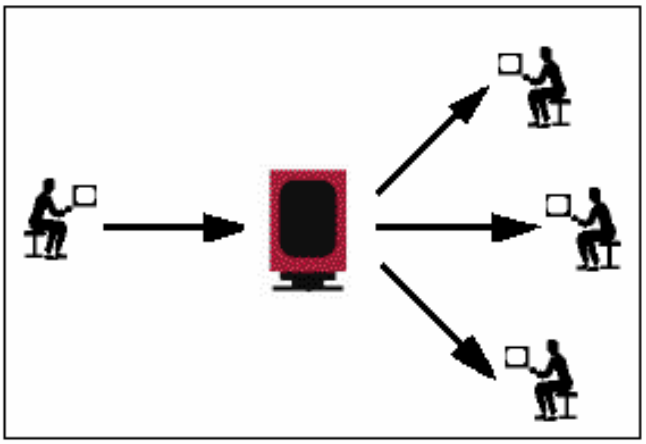
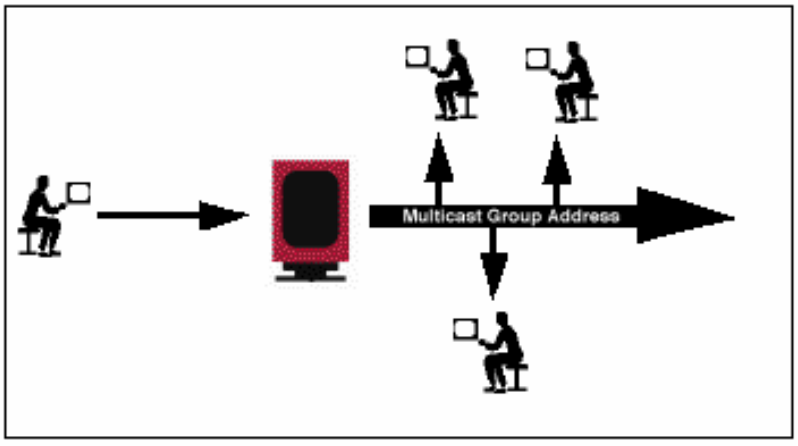


Figure B shows Conference Server distributing a single participants data stream to a multicast group address (for simplicity of illustration, we have shown communications flowing in one direction only). Notice that Conference Server only needs to send a single copy of the data stream. Any number of recipients can receive it from the multicast group address.

Figure B: Multicast Conference



The Internet and many corporate intranets are unicast environments. While the Conference Server optimizes the use of bandwidth in a unicast environment, unicast is not an efficient way to handle the demands of group multimedia communications over IP networks. With large conferences, the number of copied data streams distributed on a network can consume a lot of bandwidth. The Conference Server videoconferencing solution is multicast-capable application software. In addition, it provides a bridge between unicast and multicast environments.

To implement multicast on your network, your infrastructure must comply with the IP Multicast standard. This includes:

- TCP/IP stacks
- Network interface cards

- Computer operating systems
- Routers and switches

Vendors of these network products can help you select the appropriate hardware and software. Note that H.323 clients cannot currently take advantage of IP multicast.

To enable multicast for a conference, select the **Enable multicast** option in the **Multicast** section of the Add Conference page.

The Conference Server automatically chooses appropriate multicast group addresses and port numbers on which to route client video, audio, and control data. It also sends out a multicast session announcement that you specify to a well-known multicast address.

To enable multicast for your conference, you must also enter a time-to-live value in the **TTL** text field. TTL values control the number of routers, or "hops", that an IP multicast packet is allowed to traverse. Each time a router forwards a packet, the TTL value decrements. A multicast packet whose TTL expires (decrements to 0) is no longer forwarded. This prevents multicast packets from needlessly being forwarded to regions of the Internet that lie outside the subnets of intended participants. The table below gives the recommended TTL values for a variety of distances. These values are estimates, since you cannot determine the exact route that data will travel on the Internet. A TTL value cannot be greater than 255 or less than 1.

Table: Distance and TTL Values

Distance	**TTL**
Subnet	1
Site	15
Region	63
Continent	127
World	255

Enabling multicast lets CUseeMe protocol clients take advantage of available IP multicast on a network without giving up any conference control features. While the Conference Server routes client data streams to multicast group addresses, it continues to enforce conference parameters such as max-participants, admit and deny lists, and send and receive rates.

Self-Reflect

This option is available only on the Add CUseeMe Conference page.

To enable the self-reflect mode for a conference, select the **Allow users to view themselves** option in the **Miscellaneous** section of the Add Conference page.

The self-reflect mode lets CUseeMe protocol participants test the quality of their connection to the Conference Server. If you enable the self-reflect mode in a conference, clients that use the CUseeMe protocol see themselves listed in the Participants List of their client application. They can choose to receive their own local video stream in a remote video window and hear their own audio. This allows CUseeMe protocol participants to adjust their settings before joining another conference.

Root

To enable **Root** mode for a conference, select the **Set this conference as a Root**

conference option in the **Miscellaneous** section of the Add Conference page.

The Root mode is included for administrative purposes. Participants in a Root conference become participants of all other conferences on the server simultaneously.

RADVISION recommends that you assign the Private attribute to Root conferences. You can use a password and require authentication in order to make the conference secure and restrict it to administrators only.

You can have only one Root conference on a Conference Server. You cannot link Root conferences between Conference Servers.

Enable tracking

To enable tracking, select **Enable tracking** option in the **Miscellaneous** section of the Add Conference page.

When you enable tracking, the Conference Server creates a track file for the conference. The track file keeps session data about all client connections to that conference. This is the same information that the Conference Server sends to the RADIUS server for billing purposes (for more information, see **Interfacing with Third-Party Billing Systems**). Typically, the information in the track file is not used directly for billing purposes. You can use it for cost analysis or future billing considerations.

By default, the Conference Server names track files in the format **cs<id>.trk** where <id> is the ID number of the conference that you tracked. For example, the track file for conference 16 would be **cs16.trk**. Also by default, the Conference Server saves track files in the installation directory of the administrative server for the domain.

You can also define your own file name and/or directory path. Enter the file name and directory path in the **Files** field adjacent to the **Enable tracking** option. The directory that you specify must reside in the installation directory. Do not enter spaces in the file name or directory path.

For example, specifying

```
your_directory\sports_chat.trk
```

creates the track file for a Windows installation in

```
C:\Program Files\Click to Meet\Conference Server
7.X.X\your_directory\sports_chat.trk
```

For a Unix or Linux installation, it creates the track file in

```
/usr/local/ctm/confsrv/your_directory/sports_chat.trk
```

The Conference Server includes session data in the track file as follows:

```
Client Session Track Record {Rev 0.2}

 Conference   : 0
 IP Address   : 100.20.30.40
 Username     : TheAccountUsername
 Password     : ********
 Start Time   : Mon Nov 29 09:30:33 2004
 Elapsed Time : 00:00:44
 Stop Time    : Mon Nov 29 09:31:17 2004
 Stop Reason  : Normal Disconnect
 Bytes Sent   : 1379
```

If you specify a new name for the track file but do not specify a new directory path, the Conference Server saves the custom-named track file in the default directory. If you define a

new directory path, but not a new name, the Conference Server will save the track file with the default name (cs<id>.trk) in the directory you specify.

Streaming

This option is available only on the Add H.323 Conference page.

To enable streaming video for your conference, select the **Streaming** option in the **Miscellaneous** section of the Add Conference page. You can add or remove video streaming for specific IP addresses. You must have the appropriate license option to enable this setting. RADVISION also recommends that you use the default video and audio port settings.

To add streaming to a conference:

1. Click **Add**. A dialog box displays that prompts you to enter the destination IP addresses for the video stream.
2. Enter the destination IP addresses for the video stream. This is the IP address where you want the video to display.
3. Enter the video and audio port settings.

If you want to edit streaming in a conference, select the conference that you want to edit and click **Edit**. If you want to disable streaming in a conference, select the destination IP address (the IP address where you do not want the video to display) and click **Remove**.

H.263+ Annexes

To enable the H.263 annexes mode for a conference, enter a selection in the **H.263+ Annexes** section of the Add Conference page. The Conference Server supports **F** and **P5** annexes. You can separate entries with a space.

For example:

F P5

Note: You must select H.263 annexes when you use the H.263+ video codec.

Editing a Conference Configuration

To edit a conference configuration:

1. Click **Conferences** on the Conference Server entry page. You can also click the **Conferences** icon in the main navigation bar. The **Conferences** page displays.
2. Select the conference you want to edit. Click **Edit**. The **Edit Conference** page displays. This page presents the same series of configuration settings as the Add Conference page. However, on the Edit Conference page the fields are filled in with the settings of the conference you have chosen to edit. You can edit any or all of the settings with the exception of **Conference ID**. For a description of each setting, see Basic Settings and Optional/Advanced Settings.
3. Enter the changes you want to make to the settings. You can edit any setting except **Conference ID**. For a description of each setting, see **Basic Settings** and **Optional/Advanced Settings**.
4. If you do not want to edit the layout, click **Finish**. The Conference Server displays a confirmation of your edits. If you want to edit the server layout, click **Next**. (The Conference Server layout defines which servers are hosting the conference and the links that exist between them, if any. For more information, see **Defining a Server Layout for Your Conference**.)

5. Enter the changes you want to make to the layout. Click **Apply.**
6. The Conference Server prompts you to save the conference and the layout. You can :
    - Apply this server layout and save the conference
    - Save this conference with the original layout
7. Click **OK**. The Conference Server displays a confirmation.

Copying a Conference Configuration

You can copy an existing conference configuration in order to create a new conference with the same settings. When you copy a conference, the Conference Server Administrator Web page removes the gkep-alias and gkep-confnickname settings from the copy. The original conference remains unchanged. You must issue the Telnet gkep-alias and gkep-confnickname commands to ensure that the nickname and alias settings for the new conference are unique and server-wide.

To copy the configuration of an existing conference:

1. On the Conference Server entry page, click **Conferences**. You can also click the **Conferences** icon in the main navigation bar. The **Conferences** page displays.
2. Select the conference you want to copy. Click **Copy**. The **Copy Conference** page displays.
3. Enter the changes you want to make to the settings. You can edit any or all conference settings, or leave them unchanged. Minimally, you *must* provide a unique Conference ID. If you try to submit the conference without a unique Conference ID, the Conference Server returns an error and does not save the conference. For a description of each setting, see **Basic Settings** and **Optional/Advanced Settings**.
4. If you do not want to edit the layout, click **Finish**. The Conference Server displays a confirmation that it copied the conference. If you want to edit the server layout, click **Next**. (The Conference Server layout defines which servers are hosting the conference and the links that exist between them, if any. For more information, see **Defining a Server Layout for Your Conference**.)
5. Enter the changes you want to make to the layout. Click **Apply.**
6. The Conference Server prompts you to save the conference and the layout. You can :
    1. Apply this server layout and save the conference
    2. Save this conference with the original layout
7. Click **OK**. The Conference Server displays a confirmation.

Removing a conference

To remove a conference:

1. Click **Conferences** on the Conference Server entry page. You can also click the **Conferences** icon in the main navigation bar. The **Conferences** page displays.
2. Select the conference you want to remove. Click **Remove**. The Conference Server prompts you to confirm that you want to delete the conference.

3. Click **OK**.

You can define a user as being associated with a conference in the Conference Administrator database. However, when you remove a conference, you also remove the association with the user. The user record remains in the database.

The Conference Server Layout Applet

The Conference Server layout applet has two primary sections: a toolbar and a mapping area. The mapping area provides a place where you can graphically represent, or map out, your Conference Server layout. You can also apply a template to the layout.

Working with the Conference Server Layout Applet

The Conference Server layout defines the server or servers that host a conference and how data flows between them. The Conference Server lets you create templates that define the layouts. You can use these templates to save you the work of redefining the connections. For example, you may frequently set up small, interactive videoconferences between your corporate office and two remote offices. If you have a Conference Server at each location, you can specify the links between the three servers, save it as a template, and use it each time you set up a conference of the same type.

You can access the Conference Server layout applet from the **Network** area and from the **Conferences** area. From the Network area, you use the applet to create and save layout templates. From the Conferences area, you use it to apply a layout to a conference. When you add or edit a conference in the Conferences area, you can select a template or define a new, customized layout.

The applet has two main sections: the mapping area and the toolbar.

The Mapping Area

The mapping area provides a place where you can graphically represent, or map out, the Conference Server layout. From within the applet you can define which Conference Servers to link and the flow of data between them. If you want to host a conference on a single Conference Server, you need to create a layout with a single server configuration.

The Toolbar

The Conference Server Layout Applet toolbar features the following tools:

Selection Tool

Click the Selection Tool to put the pointer in selection mode. You can select the icons and place them in the mapping area. You can also edit, delete, and move them.

Conference Server Tool

Click the Conference Server Tool to place a new Conference Server icon in the mapping area.

Multicast Tool

Click the Multicast Tool to place a multicast icon in the mapping area. The multicast icon represents a multicast group address, or node.

Uni-Directional Link Tool

Click the Uni-Directional Link Tool to create a one-way link between two Conference Servers or between a Conference Server and a multicast group address. When you use the uni-

directional link tool, data flows in only one direction between Conference Servers.

Bi-Directional Link Tool

Click the Bi-Directional Link Tool to create a two-way link between two Conference Servers or between a Conference Server and a multicast group address. When you use the bi-directional link tool, data flows in both directions between Conference Servers.

Top Provider Tool

Click the Top Provider Tool to designate a Conference Server in your layout as the top provider for your H.323 conference. The top provider creates the initial T.120 conference and then invites linked servers to create matching T.120 conferences.

Load Button

Click the Load button to load a previously saved layout template in the mapping area. You can also click the Load button to clear the mapping area and create a new layout.

Save Button

Click the Save button to save your Conference Server layout as a template. This button displays only in the layout applet in the Network area.

Delete Button

Click the Delete button to delete a previously saved template from the server. This button displays only in the layout applet in the Network area.

Quit/Apply Button

Click the Quit button to close the layout applet. In the Network area, the Conference Server prompts you to save your layout as a template. In the Conferences area, the Conference Server prompts you to apply the layout to your conference.

Defining a Server Layout for Your Conference

The Conference Server displays the **Define Conference Server Layout** page when you click **Next** on the **Add Conference** page (after you specify your conference settings.) You can create a new server layout or apply a previously defined server layout template.

A Conference Servers does not have to be in your domain to be included in the layout. However, if you include a server that is not in your domain, you must make sure that server is set up properly to participate in the link. For example, you can create a conference on CS A (CS = Conference Server) with a uni-directional link from CS A to CS B. If CS B is not in the same domain as CS A, a complimentary conference must be set up on CS B. This complimentary conference also must specify the uni-directional link from CS A to CS B.

To define a server layout for your conference:

1. Click the **Conference Server Tool** in the layout applet toolbar.
2. Click once anywhere in the mapping area. The **Add a CS** (CS = Conference Server) window displays.
3. From the drop-down list, choose a Conference Server in the domain. You can also click **More** to choose a Conference Server from another domain.

   If the Conference Server that you want to use for your template does not display in

the drop-down list, click **Other**. The **Add a New CS** window displays.

4. Enter the host name or IP address of the Conference Server that you want to add for your template. Click **OK**. The new Conference Server name displays as the selected option in the drop-down menu of the first dialog box.
5. Click **OK**. An icon representing the Conference Server you chose displays in the mapping area.

You can add additional Conference Servers to the layout or to the template. Each time you add a server to the layout or to the template, an additional Conference Server icon displays in the mapping area. You can double-click any Conference Server icon to change the server or delete it from the layout or the template.

Click **More** in the **Add a CS** applet window to display information about the links for each conference on the server you selected.

Linking Data Streams

You can define how data streams flow between Conference Servers. You can create a uni-directional (one-way) or bi-directional (two-way) link between any two Conference Servers. These links are unicast connections unless you specify a multicast connection. For more information, see **Unicast and Multicast**.

Multicast Linking

To extend a multicast connection over the Internet, you must use a network such as the MBONE (Multicast Backbone). The MBONE is a multicast network layered on top of the Internet.

To choose multicast linking between the servers hosting your conference:

1. Click the **Multicast Tool** in the layout applet toolbar.
2. Click once in the mapping area. The **Add a Multicast IP** applet window displays.
3. Enter the **multicast group address** that you want to add for use in your template. This address must be between **224.0.0.1** and **239.255.255.255**.
4. Enter appropriate values for **Port number** and **TTL** (time-to-live).
5. Click **OK**. An icon representing a multicast group address displays in the mapping area.

Double-click any multicast icon to change the multicast address or parameters. You can also double-click to delete it.

Port Numbers

The **port number** parameter is the channel or gateway by which data streams to and from the multicast group address. When you use multicast to link Conference Servers, you must choose an even-valued port number between **32768** and **49150**. You must specify the same port number for all participating Conference Servers.

The Conference Server uses the port you specify to send connection information. It automatically opens a second port (16K less than the port specified) to send RTP audio. It also automatically opens a third port (also 16K larger than the port specified) to send RTP video.

Note: If you have two or more nodes in a multicast conference, use the same multicast address and port number for all nodes. Do not use port number 40406, as this causes problems with multicast conferences.

Time to Live Value

The **TTL** value controls the number of routers, or “hops”, that an IP multicast packet is allowed to traverse. Each time a router forwards a packet, the TTL value decrements. When the TTL of a multicast packet expires (decrements to 0), the Conference Server no longer forwards it. This prevents the Conference Server from needlessly forwarding multicast packets to regions outside the subnets of intended participants.

The following table gives recommended TTL values for a variety of distances.

Table: Distance and Recommended TTL Values

Distance	**TTL**
Subnet	1
Site	15
Region	63
Continent	127
World	255

The TTL value cannot be greater than 255 or less than 1. Unless the TTL value is greater than 15, the multicast router does not forward data streams beyond your LAN. The recommended TTL values in the table are estimates, since you cannot determine the exact route of data on the Internet. You can specify a TTL value only if the data streams travel *from* a Conference Server *to* a multicast group address. If a Conference Server receives data streams from a multicast group address but does not send data streams back to that address, you do not need to enter a TTL value.

The TTL field in the Add a Multicast IP window is the TTL for all links connected to this multicast IP address. All servers that you link to this multicast address take this TTL value.

To change the TTL value, click the Selection Tool and then double-click the multicast icon you want to edit. An applet window displays that allows you to edit the multicast group address parameters, including the TTL.

If you want the TTL value of the multicast group address to display in the mapping area, click **Display TTL**.

Creating a Uni-Directional or Bi-Directional Link

1. Click the **Uni-Directional Link Tool** or the **Bi-Directional Link Tool** in the layout applet toolbar.
2. Select a Conference Server icon in the mapping area.
3. Click the icon and drag your mouse to another Conference Server icon or to a multicast icon. A green line with an arrow at one or both ends (signifying a one-way or two-way link) displays between the two icons.
4. Repeat Step 8 to define the links between each of the Conference Servers and multicast group addresses that you have specified in your layout.
5. Click **OK**.

The following table explains the link colors.

Table: Link Colors

Link Color	Description	Media Supported
Green	Selected link	Not applicable
Red	Multicast bi-directional* or uni-directional link	Audio and Video (AV) only
Blue (default)	Unicast bi-directional or uni-directional link	Audio, Video, and T.120* (AVT)
Magenta	Unicast bi-directional link	Audio and Video (AV) only
Yellow	Unicast bi-directional link	T.120 (T) only

*T.120 protocol is capable only over a bi-directional link.

Changing Linking Settings

You can double-click any link to change its direction, change its parameters, or delete it. For more information, see the figures for the uni-directional dialog box and the bi-directional dialog box.

When you edit a link between two servers, you can specify the following items:

- Send Rate - How much bandwidth a server can use to transmit data to a linked server
- Keep-Alive Interval - How often a server sends keep-alive messages to a linked server
- Media - The media supported by the link

One-Way Link

If the link is one-way, you can edit the **Send Rate** only for the primary server (the server that sends conferencing data). The secondary server (the receiving server) sends the keep-alive messages. One-way links are capable of Audio and Video (AV) only.

Two-Way Link

If the link is a two-way link (in which conferencing data flows in both directions between servers), you can edit the **Send Rate** and **Keep-Alive Interval** for both servers. By default, the Conference Server sets the Send Rate to 1544 Kbps for data sent between servers.

Two-way links support three combinations of media. You can choose:

- T.120 (T) only
- Audio and Video (AV) only
- Audio, Video, and T.120 (AVT)

Multi-Conference Links

If you link more than one conference between two servers, the Conference Server adds the amount of bandwidth you designate for each conference. Conferences share the cumulative amount of bandwidth on a first-come, first-served basis. If you have a low total bandwidth, each conference may not receive the bandwidth that you specify in the Send Rate.

Keep-Alive Messages

Keep-alive messages allow linked servers to communicate when no conferencing data is being sent. By default, the Conference Server sets the keep-alive interval to four seconds, which is satisfactory for most conferencing situations. However, you can change the keep-alive interval. For example, if your servers are linked over a costly ISDN connection, you may not want to keep the connection open if no conferencing data is being sent. In this case, you can increase the keep-alive interval so that the connection closes when no conferencing data is being sent.

Designating a Top Provider

If you create an H.323 conference and link it between multiple Conference Servers, you must designate one of the Conference Servers as the top provider. The server you designate as the top provider determines the order in which T.120 conferences are created on linked servers.

A linked server does not create a T.120 conference until another server invites it to do so. The top provider creates the first T.120 conference and then invites any servers that are directly linked to it to create matching T.120 conferences. Those servers, in turn, invite any additional servers to which they are directly linked. This continues until all the linked servers hosting the H.323 conference have matching T.120 conferences.

To designate a Conference Server as top provider in your Conference Server layout:

1. Click the **Top Provider Tool** in the layout applet toolbar.
2. Click the icon for the Conference Server you want as your top provider. The word **TOP** displays directly above the Conference Server icon.
3. Click **OK**.

To clear the top provider selection, click the Conference Server icon again with the **Top Provider Tool** selected. The TOP label disappears.

You can base the selection of top provider on a number of criteria such as reliability of the server system, available bandwidth, and accessibility. Explicit knowledge of the sequence in which linked T.120 conferences are created is helpful for troubleshooting purposes. If you choose not to designate a top provider, the Conference Server automatically assigns the server with the lowest IP address as the top provider.

Clearing the Mapping Area

To clear the mapping area:

1. Click the Load button in the layout applet toolbar. The **Open a layout** applet window displays.
2. Click **Create a new one**.
3. Click **OK**. The Conference Server clears the mapping area.

Changing Layout Settings

You can modify the settings for any of the icons or links in the mapping area. To change layout settings:

1. Click the **Selection Tool** in the layout applet toolbar.
2. Double click the link or icon you want to edit. An applet window displays.

3. Make the changes you want to the layout.
4. Click **OK**.

Creating a Conference Server Layout Template

You can save layouts that you create in the Network area as templates. To create a Conference Server layout template:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page appears.
2. Click the **Layouts** button on the Network page. The **Define Conference Server Layout Template** page displays.
3. Choose the configuration settings that you want for the layout template.
4. When you are satisfied with the configuration you have created in the mapping area, click the **Save** button in the layout applet toolbar. The **Save As** applet window displays.
5. Enter a name for the layout template and click **Save**. This saves the layout on the administrative server as a template.

You can apply any layout that you save as a template. However, you must create the layout and save it in the **Network** area. The **Save** button does not display in the layout applet toolbar in the **Conferences** area.

Editing an Existing Template

To edit an existing template:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page appears.
2. Click the **Layouts** button on the Network page. The **Define Conference Server Layout Template** page displays.
3. Click the **Load** button in the layout applet toolbar. The **Open a layout** applet window displays.
4. From the drop-down menu, select the template you want to edit.
5. Click **OK**. The template loads in the mapping area where you can view its details and edit its configuration.
6. When you finish changing the template, click **Apply**. This saves the changes to the template.
7. Click **OK**.

You must edit templates from the Network area. The Conference Server applies the changes you make in the layout applet to the conference but does not save them to the template itself. To edit a template permanently, you must use the layout applet in the Network area

From the **Open a layout** window, you can also choose to create a new layout. If you select this option and click **OK**, the mapping area is cleared.

Deleting an Existing Template

To delete a template from the server:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page appears.
2. Click the **Layouts** button on the Network page. The **Define Conference Server Layout Template** page displays.
3. From the drop-down menu, select the template that you want to delete.
4. Click the **Delete** button in the layout applet toolbar. The **Delete a layout from the server** applet window displays.
5. Click **Delete** in the applet window. The Conference Server confirms that you want to delete the template.
6. Click **Delete** again. The Conference Server deletes the template from the server.

You must delete templates in the **Network** area. The **Delete** button does not display in the layout applet toolbar in the **Conferences** area.

Applying a Template to the Layout of a Conference

From the **Open a Layout** window, you can load a server layout template that you previously defined in the Network area.

To apply a template to the layout of a conference:

1. Click the **Network** button on the Conference Server entry page. You can also click the **Network** icon in the main navigation bar. The **Network** page appears.
2. Click the **Layouts** button on the Network page. The **Define Conference Server Layout Template** page displays.
3. Click **Select it from the list**. Choose the template you want from the drop-down list.
4. Click **OK**. The Conference Server loads the template in the mapping area where you can view its details and edit its configuration.
5. Click the **Apply** button in the layout applet toolbar. The **Save this conference** applet window displays.
6. Click **Apply this layout and save the conference**.
7. Click **OK**.

Avoiding Conference Server Layout Conflicts

The Conference Server requires that all conferences linked between two servers share the same link type and bandwidth. For example, you use the **Uni-Directional Tool** in the Conference Server layout applet to connect CS A and CS B for Conference 1 (CS = Conference Server). You then decide to link Conference 3 between the same two servers. Since you have already established a uni-directional link from CS A to CS B for Conference 1, you must use a uni-directional link for Conference 3. However, if you choose to link Conference 3 between CS A and a different server, say CS C, you can choose a different link type and/or bandwidth.

The layout applet provides information to help you avoid creating conflicting links between servers. To view this data, click the **Conference Server Tool** in the layout applet toolbar. Click once anywhere in the mapping area. The **Add a CS** (CS = Conference Server) applet window displays. Select a Conference Server from the drop-down menu and click **More**. The **Message** applet window displays. The window contains a text box with information describing the links for each conference on the server that you selected. Uni-directional

links are represented by the word **to**. Bi-directional links are represented by the word **between**. This information helps you to avoid creating layouts with conflicting links. However, if you do inadvertently create a layout with a conflicting link and try to apply it to a conference, the Conference Server displays an error. You cannot save or apply the layout until you remove the conflicting link.

Managing User Access to Conferences

The following sections provide information on managing users to enable smooth conference performance. You can set permission levels in order to control user access to conferences.

The Users Area

The Conference Server lets you control access to conferences through the Conference Administrator database. The database installs and integrates completely with the Conference Administrator Web pages. Although you can install the Conference Administrator Web pages on multiple computers, only a single database can serve the domain. When you set up a domain, you specify which server maintains the user database. When you make a change to the user database, the database forwards the change to all Conference Servers in the domain.

The Conference Administrator database does not keep a record of every user that connects to your Conference Server. Rather, the Conference Server uses the database to maintain records of participants with special access status. This information is managed in the **Users** area of the Conference Administrator Web pages.

From the Users area, you can do the following:

- Add User Records - The **Add** button links to the **Add User Record** page. From there, you can add user records and assign special permissions.
- Search for User Records - The **Search** button links to the **Search User Database** page. From there, you can search for user records in the Conference Administrator database. With the results of your search, you can edit, copy, and remove user records.
- Create and Manage Organizations - The **Organizations** button links to the **Organizations** page. From there, you can create and manage organization records for use with the MeetingPlanner applet.
- Initialize the Database - The **Initialize** button links to the **Initialize User Database** page. From there, you can delete all user and organization records except the default administrator record.
- Backup the Database - The **Backup** button links to the **Backup User Database** page. From there, you can create a backup copy of all user records in the Conference Administrator database.

Assigning Special Permissions

Before adding or editing user records, it is helpful to understand the meaning of each special permission you can assign.

You can assign the following special permissions:

- Administrator
- Moderator
- Conference Manager
- General User
    - Normal

- Admit
- Admitted-Sender
- Deny

Administrator Permission

Administrator permission gives a user administrative access to the Conference Administrator Web pages. The Administrator permission is not specific to any conference; it applies to all conferences on your server. This allows the user with Administrator permission to configure conferences, manage a network of Conference Servers, and control user access. You can assign Administrator permission to any number of users.

To assign Administrator permission, first create a user record. Select Administrator permission and enter a username and password for authentication purposes. You do not need to know the user IP address in order to assign Administrator permission.

The default user record that installs with the database provides initial access to your server. This default record has a username of **Administrator** and a password of **changeme**. RADVISION strongly recommends that you change the username and password of this default user record as soon as possible to maintain the security of your Conference Server.

Moderator Permission

Moderator permission gives a user *limited* access to the Conference Administrator Web pages. This allows a user to control the rights of active participants in a specific conference.

To assign Moderator permission, first create a user record. Select Moderator permission and enter a username and password authentication purposes. You do not need to know the user IP address in order to assign Moderator permission.

A user with Moderator permission for a particular conference can access the **Monitor Users** page for the conference. You can do the following from the Monitor Users page:

Deny User

Add a user's IP address to Conference Server's deny list (maintained in the user database file). This disconnects the user and prevents the user from reconnecting. Users can be added to the deny list for a specific conference or to the deny list for all conferences in your domain.

Disconnect User

Temporarily disconnect a user from a conference. Participants that you disconnect are allowed to reconnect after one minute.

Grant Floor

Dynamically grant **Admitted Sender** status to a participant in the conference. When a participant is 'granted the floor' his video, audio, and chat can be seen by other members of the conference even if this is not otherwise permitted in the conference.

Revoke Floor

Dynamically revoke **Admitted Sender** status from a participant.

Set Video Source

Turn off timed or voice-switched video and force all participants in the conference to see the user selected.

Clear Video Source

Set the conference back to timed or voice-switching, as was originally selected for the conference.

The Moderator permission is very useful when you want to control participation in a conference. For example, in a distance learning environment, a professor might spend the first part of a conference giving a lecture. During the lecture it is not necessary for participants to see or hear anyone but the professor. The professor is the only admitted sender in a one-way cybercast. Later, the professor, as Moderator, can open up the conference to questions and answers from the group. The professor can select students to become temporary admitted senders. This allows all the other participants to see and/or hear these students as they ask their questions.

Note: You assign the Moderator permission on a per conference basis. Users assigned this permission can moderate a conference by logging in to Conference Server with a browser, and simultaneously joining the conference with a client conferencing application. If a Moderator is also to be an admitted sender you must create two user records: one specifying the Moderator permission, and another specifying the General User/Admitted Sender permission. Alternatively, the Moderator can 'grant the floor' to his own client from the Monitor Users page.

Conference Manager Permission

The **Conference Manager** permission gives an end user the right to access Conference Server's MeetingPlanner applet to create, schedule, edit, and remove conferences. The conferences that an end user creates with the applet are based on template conferences that have been pre-configured by an administrator. The Conference Manager permission does not allow the user to access Conference Server's Conference Administrator Web pages.

When you create a user record and assign the Conference Manager permission, you must also enter values for username, password, e-mail address, and organization. The username and password are used for authentication to Conference Server's MeetingPlanner applet. Organizations are set up in advance in the Users area of Conference Server's Conference Administrator Web pages. The organization you assign determines which template conferences will be available to the user for conference creation. The e-mail address is used as a return address when e-mail invitations for the conference are sent from the MeetingPlanner applet.

General User Permission

The **General User** permission concerns the rights of a participant in a Conference Server conference. It does not grant a user access to Conference Server's Conference Administrator Web pages. General User has meaning only in the context of the modifying permission that you select with it. The modifying permissions for General User are:

- Normal
- Admit
- Deny
- Admitted Sender

Note: **Normal**, **Admit**, **Deny**, and **Admitted Sender** can only be applied to the General User permission. They do not modify the Administrator, Moderator, or Conference Manager permissions.

General User: Normal Permission

You should assign the **General User/Normal** permission to a user record in order to allow

access to a restricted conference that uses Conference Server Username/Password authentication. This permission requires that you specify a username and password in the user record. This will enable a user to gain access to a restricted conference by first logging in with a browser to Conference Server's User Authentication Web page.

The General User/Normal permission can also be used to allow an end user *limited* access to Conference Server's MeetingPlanner applet. General users can create temporary conferences 'on-the-fly' that automatically delete after conference completion. General users cannot create scheduled or recurring conferences and cannot limit the conferences to specific participants. To enable a general user access to the MeetingPlanner applet, you must also specify a username, password, and organization. An e-mail address is optional. It is used as a return address when e-mail invitations are sent from the MeetingPlanner applet.

For more information, see Managing Organizations and Using Conference Server's MeetingPlanner Applet.

General User: Admit Permission

You should assign the **General User/Admit** permission to a user record in order to allow access to a restricted conference that uses Conference Server IP-Based authentication.

This permission requires that you specify the user's IP address in the user record. When a user attempts to connect to such a conference, Conference Server queries the user database to see if a matching user record exists. If a record exists specifying the user's IP address and the General User/Admit permission, Conference Server will allow the user to connect.

General User: Deny Permission

Conference Server maintains a deny list as part of its user database file. You should assign **General User/Deny** to a user record when you want to deny a user access to a conference(s). This permission requires that you specify the user's IP address in the user record. You can deny a user on a per conference basis or for all conferences in your domain. If a user attempts to connect to a conference for which (s)he has been denied, Conference Server will refuse the connection.

You can also deny users in real-time from within the Monitoring area of the Conference Server interface.

General User: Admitted-sender Permission

The **General User/Admitted Sender** permission allows a participant to send audio, video, and chat streams even when these data types are not otherwise permitted in a conference. For example, in a one-way cybercast you may want multiple participants to watch a single data stream as content source for the cybercast. You would configure this kind of conference with Broadcast mode enabled so that only admitted senders could send audio, video, and chat. Participants would receive data only from the content source (admitted sender) and not from other observers in the conference. You would need to create a user record assigning the General User/Admitted Sender permission to the user providing the content source. This would allow the admitted sender to override Broadcast mode for the conference. Admitted Sender will also override any single attribute (audio, video, chat), or combination of attributes, that has been disabled for a conference. This permission requires that you specify the user's IP address in the user record.

You can dynamically assign the Admitted Sender permission from within the Monitoring area of the Conference Server interface. You do this by 'granting the floor' to selected participants in a conference.

Note: Users assigned the Admitted Sender permission must be granted admit status separately if they need access to a restricted conference. Admit permission allows the user

access to a restricted conference that uses Conference Server IP-based authentication.

Conference Server's User Authentication Web Page

Conference Server provides an optional User Authentication Web page that provides control of client access to your Conference Server. It is designed to facilitate conference billing, authentication, and the routing of H.323 clients.

Note: If you are trying to launch NetMeeting from the User Authentication page and you are located behind a NAT, please contact your system administrator.

The User Authentication Web page does the following:

Provides a method to authenticate users by username and password

Authentication can be performed by the Conference Server user database or by a third-party billing/authentication system. The method used is determined by the User Authentication selection you make when you create a Conference Server conference.

Without the User Authentication Web page, Conference Server can only authenticate users by IP address. This is because CUseeMe protocol and other client conferencing applications currently have no way of passing a username and password to Conference Server directly. Authentication by IP address, however, presents a problem for users with *dynamic* IP addressing. Such a user receives a different IP address each time (s)he connects to the Internet. This IP address is taken from a pool of IP addresses assigned to the user's service provider. A username and password provide a static means of identifying and authenticating a user even when that user's IP address changes.

Provides a method for H.323 clients to select a specific conference from among multiple conferences on your Conference Server

The User Authentication Web page is one of several methods that Conference Server provides to route H.323 clients to specified conferences on your server. You can instruct H.323 client users to connect to this page with a Web browser before connecting to your Conference Server with an H.323 client application. An H.323 client user needs to fill out the form found on this page, specifying the ID number of the conference to which they want to connect (and username/password if required for the conference). Once submitted, commands are sent to Conference Server associating the user with the specified conference. When the user then connects to the Conference Server with an H.323 client application, Conference Server automatically routes the user to the conference specified in the User Authentication Web page.

When a user makes an authentication request through the User Authentication Web page, Conference Server is queried to determine the authentication method selected for the specified conference. The following list describes how the User Authentication Web page works with the various authentication methods that you can specify when creating a conference:

None

If **None** is specified under User Authentication on the Add Conference page, the conference does not require authentication. There is no need to have CUseeMe-protocol client users log in through the User Authentication Web page in this case. The page can, however, still serve to route H.323 clients to a specified conference on your Conference Server.

Note: Because Conference Server does not perform authentication checking in this case, it is not necessary to have H.323 client users fill in the Username and Password text fields.

Conference Server

If **Conference Server Username/Password** authentication is specified under User authentication on the Add Conference page, all users must log in with a browser through the User Authentication Web page before connecting to the conference with their videoconferencing client. When a user submits an authentication request, Conference Server's user database file is queried to see whether the user is allowed to participate in the conference.

Note: It is an unnecessary step to have CUseeMe protocol users log in through the User Authentication Web page if **Conference Server IP-based** authentication is being used. Conference Server will authenticate these users automatically when they connect to the conference with their client application. However, H.323 clients still benefit from the User Authentication page even with Conference Server IP-based authentication. The page serves to route H.323 clients to a specified conference on your Conference Server. Users must specify Username, Password and Conference ID.

RADIUS

If **RADIUS authentication** is specified under User Authentication on the Add Conference page, all users must log in with a browser through the User Authentication Web page before connecting to the conference with a videoconferencing client. Conference Server queries a third-party RADIUS server for user authentication. Only users authenticated by that system can connect to the conference. Users must specify Username, Password, and Conference ID in the User Authentication Web page.

For more information, see Interfacing with third-party billing systems.

The table below summarizes when users should use Conference Server's User Authentication Web page:

Table: Use of Conference Server's User Authentication Web page

Client	Authentication method
CUseeMe protocol users	Conference Server authentication by username/password RADIUS authentication
H.323 users	6. Conference routing with no authentication 7. Conference routing with IP-based Conference Server authentication 8. Conference Server authentication by username/password RADIUS authentication

For specific instructions on accessing the User Authentication Web page see the next section, "Accessing Conference Server's User Authentication Web Page."

Accessing Conference Server's User Authentication Web Page

To access the Conference Server User Authentication Web page, videoconferencing users need to follow these steps:

1. Enter the following address in a Web-browser:

```
http://<yourserver>:8080/cs/index.html
```

where <yourserver> is the IP address or the host name of the computer on which your Conference Server Conference Administrator Web pages are installed. For example, to connect to the User Authentication Web page for a public Conference Server, a user needs to

enter either of the following URLs (Universal Resource Locator) in the Web-browser:

```
http://209.143.192.6:8080/cs/cs/index.html
 http://cafe.radvision.com:8080/cs/index.html
```

2. Once connected to the Conference Server User Authentication Web page, users need to first enter the following information and then click the **Authenticate** button:

User Name (if required)

Users enter a username if the conference requires username/password authentication. Username must be specified in a user record in Conference Server's Conference Administrator database or your third-party RADIUS server.

Password (if required)

Users enter a password if the conference requires username/password authentication. Password must be specified in a user record in Conference Server's Conference Administrator database or in your third-party RADIUS server.

Choose conference from list

Users select a conference to join from the pull-down menu. The list displays all public conferences currently active in the Conference Server domain. If a conference has been given the private attribute, it will not display in the list. Use the field labeled **Specify Conference ID (if not listed)** to specify the ID of a private conference.

Specify Conference Password (if required)

If the conference is password protected, users must enter the conference password in this field. An administrator determines password protection for a conference when adding or editing a conference in the Conference area.

I want to choose the server to use

If a conference is hosted by multiple Conference Servers, Conference Server will automatically choose which server to tell the client to connect to based on load-balancing needs of the network. Users can override this by selecting the check box labeled **I want to choose the server to use**. Conference Server will display a list of servers that are hosting the conference.

I am using an H.323 compatible client

H.323 users need to select the check box labeled **I am using an H.323 compatible client**. By selecting this check box, Conference Server will associate the user to the selected conference. When the user connects with an H.323 client, Conference Server will automatically route the client into the correct conference.

If user authentication fails, Conference Server displays a Web page with a rejection message and does not allow the user to connect to the conference.

If authentication succeeds, Conference Server polls all the Conference Servers hosting the specified conference to see which has the lightest participant load. It then issues the appropriate commands to that server to allow the user to connect, and displays a Web page appropriate to the user's client.

If the user has a CUseeMe client,

a Web page displays where the user is provided the conference address for connecting to the conference from within his videoconferencing client.

If the user has an H.323 client,

a Web page displays where the user can launch NetMeeting, if appropriate, or use the conference address provided for connecting to the conference from within his

videoconferencing client.

Note:

- The user must connect to the Conference Server conference from the same IP address used to submit the authentication request. For a user with dynamic IP addressing, this means the connection to the conference must be made during the same Internet session as the authentication request.
- If the user selected the check box labeled **I want to choose the server to use,** Conference Server will not poll the servers for load balancing information. Instead, it will display a list of servers that are hosting the conference and allow the user to decide which server to connect to.

Customizing the User Authentication Web Page

The User Authentication Web page is meant to be an interface between an organization's videoconferencing service and its users.

You can modify it with custom graphics and links to reflect the identity and specific needs of your organization.

For example, your company may want to allow new customers to register online for videoconferencing services. You could add a link on Conference Server's User Authentication Web page to a secure online registration page, as well as integrate company logos and other graphics to maintain consistency with your company Web site.

User authentication

The Conference Server provides several different options to control client access to your conferences. To select one of these options, click the appropriate selection button under **User Authentication** on the Add Conference page:

None

The default selection under **User Authentication**. When None is selected, the conference does not require authentication. Users can connect freely to the conference, limited only by the settings you have specified in your conference configuration.

Conference Server authentication

RADIUS authentication

Admit Reject Message

If a CUseeMe protocol user is denied access to a conference because of failed authentication, Conference Server will send that user a refusal message. You can specify what message Conference Server will send by filling in the Admit Reject Message text field under User Authentication on the Add Conference page. For example, a company offering videoconferencing services for a fee might use the message to direct users to a Web page where they can enroll for the fee-based services. Conference Server limits the Admit Reject Message to 255 characters.

Note: A user that has been "denied" will not be able to connect regardless of which user authentication method has been selected for the conference (see Assigning special permissions).

Monitoring Conferences

The following sections provide information on monitoring conferences using Conference Server features.

The Monitoring Area

Conference Server allows you to access real-time information concerning activity on your Conference Server.

From the **Monitoring** area of Conference Server's browser-based interface, you can:

- Dynamically monitor and control client participation in an active conference. For example, you can see which participants are connected to a conference and how long they have been connected. You can also disconnect a participant from a conference, deny further access, and grant or revoke special status to participants in real-time.
- View real-time statistical information for an individual conference or for a Conference Server. Information you can obtain includes total number of users currently connected, how much data is being received, and how much data is being dropped by the network.
- Monitor Conference Server H.323 gatekeepers in your domain for information on H.323/H.320 endpoints that are currently registered.

There are two versions of the **Monitoring** area. The one you see depends on whether you log in to Conference Server as:

- Administrator
- Moderator

Using the Monitoring Area as an Administrator

While logged in to Conference Server as an Administrator you can:

Monitor users in a conference

Dynamically control client participation in an active conference or in all conferences in your Conference Server domain.

Monitor dynamic statistics for a conference

Get a real-time snapshot of client participation in a conference.

Monitor dynamic statistics for a Conference Server

Get real-time bandwidth consumption and participation statistics for a particular Conference Server in your Conference Server domain.

Monitor Conference Server H.323 gatekeeper activity

Get information on H.323/H.320 endpoints that are currently registered with Conference Server gatekeepers in your domain.

Using and Accessing the Monitoring Area as a Moderator

While logged in to Conference Server as a Moderator you can monitor users in a conference. You can also dynamically control client participation in an active conference or in all conferences in your Conference Server domain.

When you log in to Conference Server as a Moderator, you have limited access to Conference Server's Conference Administrator Web pages. Specifically, Moderators can

access a modified version of the Monitoring page. This page allows a Moderator to control client participation in an active conference. It is modified in that it does not contain links to other areas of the Conference Server interface, other than a single link to these HTML Help files.

To access the Monitor Users page as a Moderator, you must have a username and password defined in Conference Server's user database with the Moderator permission assigned (see Adding user records).

To log in as a Moderator:

1. Launch your Web browser and connect to the following URL (customized with the IP address or domain name, and HTTP port of your Conference Server Conference Administrator Web pages):

```
http://yourserver:8080/cs/cs.html
```

For example, if you installed your Conference Server on a computer with IP address **100.1.1.1** and domain name **conference.radvision.com**, you could enter either of the following URLs:

```
http://100.1.1.1:8080/cs/cs.html
```

```
http://conference.radvision.com:8080/cs.html
```

The Conference Server login applet appears in your browser window prompting you for a username and password.

Note: For Windows, there is a shortcut to this URL if you log in to Conference Server's Conference Administrator Web pages from the same computer on which they are installed. Select **Login to Conference Server** from the RADVISION --> Conference Server Programs group on the Start menu. Conference Server will launch your browser and bring you directly to the Conference Server login page.

2. In the **Username** field, enter your Moderator username (as defined in Conference Server's Conference Administrator database).
3. In the **Password** field, enter your Moderator password (as defined in Conference Server's Conference Administrator database).
4. Select **Moderator** from the pull-down menu labeled **Permission**.
5. Click **OK**. Conference Server will link you to the **Monitoring** page. The Monitoring page displays a selection box with a list of conferences to which you have been assigned the Moderator permission.
6. Select the conference you want to moderate from the selection box, and click **Monitor Users**. The **Monitor Users** page displays for the conference you selected.

Note: If you have been assigned Moderator permission for All Conferences, you can choose to monitor the participants in all conferences simultaneously or per conference.

Monitoring Users

The Monitoring page provides a selection box with a list of active conferences.

When you log in to Conference Server as a Moderator,

the list contains all those conferences to which you have been assigned Moderator status.

When you log in to Conference Server as an Administrator,

the list contains all active conferences in your Conference Server domain.

Each conference is identified by Conference Name and Conference ID. To monitor a conference, select its name from the selection box then click the **Monitor Users** button. This will link you to the **Monitor Users** page for the conference you selected.

There is an icon task bar on the Monitor Users page that allows you to control participation in a conference. The actions you can perform from the icon task bar are:

- Deny User
- Disconnect User
- Grant Floor
- Revoke Floor
- Setting a Video Source
- Clearing a Video Source

To perform any of these actions, click on a participant name in the selection box on the Monitor Users page, and then click the appropriate icon above the selection box. The participant selection box on the Monitor Users page provides the following information for each participant:

Name

The participant's username as entered in the client application.

IP address

The IP address of the computer from which the participant is connecting.

Connect Time

How long the participant has been connected to the conference.

Host Machine

The Conference Server to which the participant is connected.

Conf ID

The ID of the conference to which the participant is connected.

G

An asterisk (*) in the "G" column denotes that a user has been granted the floor (been given admitted sender status). Admitted sender status can be granted in the Users area of Conference Server's Conference Administrator database or by granting a participant the floor from the Monitor Users page in an active conference.

You can sort the list of participants by any of the information categories (Name, IP Address, Connect Time, Host Machine, Conference ID, Granted Floor). To do this, click on the appropriate category header above the participant list selection box. For example, if you want to sort users by how long they've been connected, click the **Connect Time** header above the selection box. Conference Server will arrange the participants in ascending order from shortest connect time to longest connect time.

The participant information on the Monitor Users page is current when you first access the page. To keep the information updated make sure the **Keep List Updated** check box is selected. Conference Server will update the information automatically every 90 seconds. If you want an update between 90 second intervals, click the **Reload** (Netscape Navigator) or **Refresh** (Microsoft Internet Explorer) button on your browser.

Below the participant selection box is a User Attributes key (not shown). If you click a participant's name in the selection box, Conference Server displays the following attributes for that user in the User Attributes key:

Can Send Audio

Displays whether the participant is able to send audio.

Can Receive Audio

Displays whether the participant is able to receive audio.

Is Sending Video

Displays whether the participant is sending a video image.

Granted Floor

Displays whether the participant has been granted the floor (been given admitted sender status). Admitted sender status can be granted in the Users area of Conference Server's Conference Administrator database or by granting a participant the floor from the Monitor Users page in an active conference.

Note:

- As an Administrator you can choose to monitor all conferences simultaneously. To do this choose ****All Conferences**** from the selection box on the Monitoring page, then click **Monitor Users**. Moderators can only monitor all conferences if they have been assigned this permission specifically in the user database.
- The participant selection box displays all participants connected to a selected conference across all servers, both inside and outside your Conference Server domain. However, you will not be able to apply an action (Deny, Disconnect, Grant Floor, Revoke Floor) to any participants that are connected to the conference on servers outside your domain. If you attempt to do this, Conference Server will return an error.

Disconnecting a User

The **Disconnect User** button on the Monitor Users page allows you to temporarily disconnect a user from an active conference.

To disconnect a user (if you are logged in as a Moderator, skip to Step 2):

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.
3. Select the appropriate participant from the selection box on the **Monitor Users** page, and click **Disconnect User**. An applet window will appear titled **Confirm User Disconnect**.
4. Click **Disconnect**. A second window will appear titled **Disconnect/Deny Message**.
5. Enter a message of 255 characters or less and click **OK**. Conference Server will send the participant the specified message and disconnect the participant from the conference. The user can reconnect after one minute. If you do not specify a message in the Disconnect/Deny Message window, Conference Server will send the following default message:

```
Your connection is being terminated.
```

Note: H.323 participants will be disconnected from the conference but will **not** receive the disconnect message.

Denying a User

Conference Server maintains a deny list for your Conference Server domain and for individual conferences in that domain. The **Deny User** button on the Monitor Users page allows you to place a user on a deny list while the user is participating in a conference.

To deny a user (if you are logged in as a Moderator, skip to Step 2):

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.
3. Select the appropriate participant from the selection box on the Monitor Users page, and click **Deny User**. An applet window will display titled **Confirm User Deny**.
4. Click **This** if you want to deny the user only for the conference to which the user is currently connected. Click **All** if you want to deny the user for all conferences in your Conference Server domain. A second applet window will appear titled **Disconnect/Deny Message**.
5. Enter a message of 255 characters or less in this window and click **OK**. Conference Server will send the participant the specified message and disconnect the participant from the conference. In addition, Conference Server will add the participant's IP address to the appropriate deny list and will not allow the participant to reconnect. If you do not specify a message in the Disconnect/Deny Message window, Conference Server will send the following default message:

```
You are denied access to this conference.
```

Note:

- H.323 participants will be disconnected and denied from the conference but will **not** receive the deny message.
- Another way to deny a user is to create a user record in Conference Server's user database. In the user record you must specify the user's IP address and assign the **Deny** permission. For more information on this method, see The Users area.

Granting the Floor to a User

The **Grant Floor** button on the Monitor Users page allows you to grant admitted sender status to selected participants in an active conference. When a participant is 'granted the floor', the video, audio, and chat of that participant can be seen by other members of the conference when this is not otherwise permitted in the conference.

To grant the floor to a user (if you are logged in as a Moderator, skip to Step 2):

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.

3. Select the appropriate participant from the selection box on the **Monitor Users** page, and click **Grant Floor**.

Generally, you use the Grant Floor button in a conference configured with **Broadcast** and **Allow audience to interact with sender** settings enabled. For example, a content provider may cybercast a celebrity interview over the Internet. The conference is configured so that only two data streams are seen by the audience: that of the celebrity and that of the interviewer. This is achieved by the following:

Enabling 'Broadcast' and 'Allow audience to interact with sender' settings

in the conference configuration

Creating a user record

for the interviewer assigning the Moderator permission

Creating a user record for the celebrity assigning General User/Admitted Sender status,

or having the interviewer (Moderator) grant the floor to his media stream and that of the celebrity during the conference.

Later, the interviewer (as Moderator) opens up the conference to questions from the audience by 'granting the floor' to selected audience members. As the selected audience members asks questions of the celebrity, they can be seen and heard by other audience members.

Note: In order for Grant Floor (or Revoke Floor) to work, the conference must be configured so that participants cannot send audio, video, or chat unless they have admitted sender status. You can achieve this for a conference in three different ways. They are:

- Enabling the **Broadcast** setting in the conference configuration.
- Enabling the **Broadcast** and **Allow audience to interact with sender** settings in the conference configuration
- Disabling the **Video**, **Audio**, and **Chat** attributes in the conference configuration

Each of these options has different applications. For more information on this see Conference Attributes and Broadcast Mode.

Revoking the Floor from a User

Revoke Floor is the complementary action to **Grant Floor**. The Revoke Floor button on the Monitor Users page is used to revoke temporary admitted-sender status from selected participants in an active conference.

To revoke the floor from a user (if you are logged in as a Moderator, skip to Step 2):

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.
3. Select the appropriate participant from the participants selection box on the Monitor Users page, and click **Revoke Floor**. The participant's video, audio, and/or chat can no longer be seen by observers in the conference.

Note: In order for Revoke Floor (or Grant Floor) to work, the conference must be configured so that participants cannot send audio, video, or chat unless they have admitted sender status. You can achieve this for a conference in three different ways. They are:

- Enabling the **Broadcast** setting in the conference configuration
- Enabling the **Broadcast** and **Allow audience to interact with sender** settings in the

conference configuration

- Disabling the **Video**, **Audio**, and **Chat** attributes in the conference configuration

Each of these options has different applications. For more information on this see Conference Attributes and Broadcast Mode.

Setting/clearing Video Sources

Conference Server allows you to set and clear the video sources for your Conference Server domain and for individual conferences in that domain. The **Set Video Source** and **Clear Video Source** buttons on the Monitor Users page allow you to either set a selected user as the video source for a conference or clear the video sources for a user while the user is participating in a conference.

To set a video source:

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.
3. Select the appropriate participant from the selection box on the Monitor Users page, and click **Set Video Source**. An applet window will display titled **Confirm User Set Video Source**.
4. Click **OK** if you want to set the selected user as the video source for the conference. Click **Cancel** if you want to abandon the applet and return to the Monitor Users window.

To clear a video source:

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Select the conference you want to monitor from the conference selection box on the Monitoring page, and click **Monitor Users**. The **Monitor Users** page displays.
3. Select the appropriate participant from the selection box on the Monitor Users page, and click **Clear Video Source**. An applet window will display titled **Confirm User Clear** Video Source.
4. Click **OK** if you want to clear the video source for the conference. Click **Cancel** if you want to abandon the applet and return to the Monitor Users window.

Monitoring Dynamic Statistics for a Conference

To obtain a real-time snapshot of client participation in a specific conference:

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page displays.
2. Click the selection button labeled **For a Conference** under **Dynamic Statistics** on the **Monitoring** page.
3. From the pull-down menu, select the conference for which you want statistics and click **Get Statistics**. Conference Server will link you to the **Monitor Statistics** page and display the following information for the conference you selected:

- Number of servers hosting the conference and, of these servers, how many are ***not*** in your Conference Server domain.
- Number of participants currently connected to the conference across all servers in your

Conference Server domain.

- Individual reports for each server in your Conference Server domain, reporting number of participants connected to the conference locally and the average amount of time participants have spent connected. Conference Server displays connect time in HH:MM:SS format, where HH = hours, MM = minutes, and SS = seconds.

You can update the conference statistics at any time by clicking the **Refresh** button at the bottom of the Monitor Statistics page.

Note: In order for dynamic statistics to work, you must set the interval at which Conference Server logs *historical* statistics to an integer greater than 0. You do this when you add (or edit) a Conference Server to your Conference Server domain. See Historical Statistics for more information on this.

Monitoring Dynamic Statistics for a Conference Server

To obtain bandwidth and participation statistics for a specific server in your Conference Server domain:

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring** icon that displays in the main navigation bar. The **Monitoring** page appears.

2. Click the selection button labeled **For a Server** under **Dynamic Statistics** on the **Monitoring** page.

3. From the pull-down menu, select the Conference Server for which you want statistics and click **Get Statistics**. Conference Server will link you to the **Monitor Statistics** page and display the following information for all conferences on the server you selected:

- Total number of participants currently connected.
    - This is further broken down to show participants that are connected directly to the server (local) and participants that are connected indirectly by way of linked servers from which the local server is receiving data.
- Average amount of data Conference Server received from clients during the last monitoring period, including clients on linked servers.
- Average amount of data Conference Server forwarded to clients during the last monitoring period, including clients on linked servers.
- Average amount of data Conference Server pruned (intelligently discarding because of bandwidth limitations) during the last monitoring period.
- Average amount of data Conference Server was unable to send because it was dropped by the network during the last monitoring period.
- Data amounts are in megabits (MB) per second. You can update the statistics at any time by clicking the **Refresh** button at the bottom of the Monitor Statistics page.

Note: In order for dynamic statistics to work, you must set the interval at which Conference Server logs *historical* statistics to an integer greater than 0. You do this when you add (or edit) a Conference Server to your Conference Server domain. See Historical Statistics for more information on this.

Monitoring Gatekeeper Activity

To obtain information on H.323/H.320 endpoints registered with Conference Server gatekeepers in your domain:

1. Click the **Monitoring** icon on the Conference Server entry page or click the **Monitoring**

icon that displays in the main navigation bar. The **Monitoring** page displays.

2. From the pull-down menu labeled **For a Gatekeeper**, select the Conference Server gatekeeper for which you want statistics.

3. Click **Monitor Gatekeeper**. Conference Server will link you to the **Monitor Gatekeeper** page and display the following information for each endpoint registered with the gatekeeper you selected:

Endpoint

The unique endpoint identifier that Conference Server assigns to each H.323/H.320 endpoint when it registers with Conference Server's local gatekeeper.

RAS Addr

The address that the Conference Server gatekeeper uses for RAS (Registration, Admission, and Status) messages with a registered endpoint. Endpoints provide this information to Conference Server's gatekeeper when they register with it. It consists of the endpoint's IP address and the port number the endpoint is listening on for RAS messaging.

EP Type

Indicates whether the endpoint is an H.323 or H.320 endpoint.

Alias

The terminal alias the endpoint provides as identification to the gatekeeper. Conference Server registers with the gatekeeper an E164 and an H323-ID terminal alias for each of its conferences. Client endpoints specify these Conference Server conference aliases as a means of connecting to a specific Conference Server conference. Client endpoints also each register their own terminal alias as identification to the gatekeeper when they connect.

Alias Type

Indicates what type of terminal alias the endpoint has provided as identification to the gatekeeper. The alias type can be any of the following:

E164

Sequence of characters (0123456789#*,) up to 128 bytes in length. H.320 clients use E164 terminal aliases.

H323ID

Sequence of any alphanumeric symbol up to 128 bytes in length. H.323 clients generally use H.323 terminal aliases.

URL

Sequence of any alphanumeric symbol up to 512 bytes in length, in the form of a Web site URL.

E-MAIL

Sequence of any alphanumeric symbol up to 512 bytes in length, in the form of an e-mail address.

XPort

A transport address in the format of an IP address and port value.

PartyNo

Sequence of characters (01234567689#*,) up to 128 bytes in length, containing a

PartyNumber prefix.

To remove an endpoint from the gatekeeper's list of registered endpoints, select the check box next to the endpoint you want to remove and click **Remove Selected**. Click **Remove All** to the clear the gatekeeper of registered endpoints.

Note:

- Conference Server provides this information only if you are using Conference Server's integrated H.323 gatekeeper. This monitoring function is not available when Conference Server is registered as an endpoint with a third-party gatekeeper.
- Conference Server registers as a single endpoint with the gatekeeper and, at the same time, registers both an H323-ID and an E164 terminal alias for each of its H.323-enabled conferences. If you remove Conference Server from the list of registered endpoints, you remove registration of all its associated conference (terminal) aliases.
- Conferencing clients that do not use RAS (Registration, Admission, and Status) messaging protocol will not appear as registered participants on the Monitor Gatekeeper page. These clients do not register with an H.323 gatekeeper.

Doing More with Conference Server

The following sections provide information on enhancing Conference Server performance and operations.

Administrative Server

The administrative server maintains the master conference configuration file (**cs.cfg**) for your Conference Server domain. Conference Server's Conference Administrator Web pages use this file as a point of reference for all conference configuration information. For example, the Conference list that displays on the top-level Conferences page is obtained from the administrative server's configuration file. This same file is used to synchronize the configuration files of your Conference Server domain members in the Network area of the Conference Administrator Web pages.

The administrative server is designated on the Add Domain Member page by a check box labeled **This Conference Server contains the master conference list**. During the installation process, you determine which Conference Server will serve as administrative server to the Conference Server you are installing (see Installing your Conference Server).

To change the administrative server for your domain:

1. Select the current administrative server from the domain member selection box on the **Conference Server Domain Members** page, and click the **Edit** button. The **Edit Domain Member** page displays.
2. Clear the check box labeled **This Conference Server contains the master conference list**. Scroll to the bottom of the page and click **Submit**. A confirmation page displays.
3. Click the **Members** button to return to the **Conference Server Domain Members** page. Select the server you want as your new administrative server from the Conference Server selection box, and click **Edit**. The **Edit Domain Member** page displays.
4. Select the check box labeled **This Conference Server contains the master conference list**. Scroll to the bottom of the page and click **Submit**. A confirmation page displays.

There may be times when you want to remove a Conference Server from one Conference Server domain and assign it to another.

To remove a Conference Server from one domain and assign it to another:

1. Log in with your browser to the Conference Administrator Web pages that control the Conference Server you want to re-assign. Navigate to the **Define Database Server** page in the Network area.
2. Enter the IP address and HTTP port number of the Conference Administrator database that controls the domain to which you want to re-assign the server. Click **Submit**. The following message displays: "Database server has been successfully changed. Please re-log back into the system."
3. Click on the **Conference Server** icon at the top left corner of your browser window to return to the Conference Server entry page, and click the **Log Out** button. A page displays confirming your log out.
4. Log in to the Conference Administrator Web pages for the domain to which you are reassigning the server. The entry page displays for Conference Server's Conference Administrator Web pages.

Note: You must have a valid user name and password in the Conference Administrator

database that controls the new domain.

5. Navigate to the **Conference Server Domain Members** page in the Network area. Click the **Add** button above the domain members list. The **Add Domain Member** page displays.
6. Fill in the server-wide settings for the Conference Server you are re-assigning. At a minimum you are required to enter values for Name, IP address, Maximum simultaneous participants allowed, and Send and Receive rate fields. Click **OK**.
7. A confirmation page displays.

Your Conference Server is now part of a new Conference Server domain and will receive its conference configuration and user access information from the administrative server and Conference Administrator database for that domain.

Using Conference Server's Continuous Presence Mode applet

Conference Server's Continuous Presence Mode applet is a Java applet that allows a conference moderator or Conference Server administrator to control which participant's video is displayed in each cell of an H.323 continuous presence video stream. By default, the videos that display are determined by Conference Server's audio-based video switching mechanism. The Continuous Presence Mode applet allows you to override this default switching on a cell-by-cell basis. It allows you to "pin" a participant's video to a particular quadrant of a continuous presence stream. When a quadrant has been pinned, it is no longer affected by default video switching. The participant's video remains constant in the quadrant, regardless of who speaks in the conference.

The Continuous Presence Mode applet allows you to pin any or all cells. Any cell that you do not pin continues to receive video based on default switching for the conference.

In order to use Conference Server's Continuous Presence Mode applet you must do the following in advance:

1. Purchase the Continuous Presence Mode option for your Conference Server. Install Conference Server and enter the Continuous Presence Mode option serial number during installation.

2. Create an H.323 conference with the H261.CP4 codec specified as the required video codec. Specifying the H261.CP4 codec enables continuous presence for the conference.

Note: Configuring a continuous presence conference should be done through Conference Server's Conference Administrator Web pages rather than through Telnet, because of the complex bandwidth issues associated with continuous presence. When you have Conference Server's Continuous Presence option installed and create a conference with H261.CP4 as the required codec, Conference Server's Conference Administrator Web pages will correctly set the send and receive rates for the conference.

3. Create a user record in the Conference Administrator database with a user name and password. Assign the user record Moderator or Administrator status for the continuous presence mode conference you created.

Note: Administrators can by default use the Continuous Presence Mode applet for any H.323 continuous presence conference in your domain. Moderators can only use the applet for those conferences you specifically assign in the user record.

To access Conference Server's Continuous Presence Mode applet, launch your Web browser and connect to the following URL:

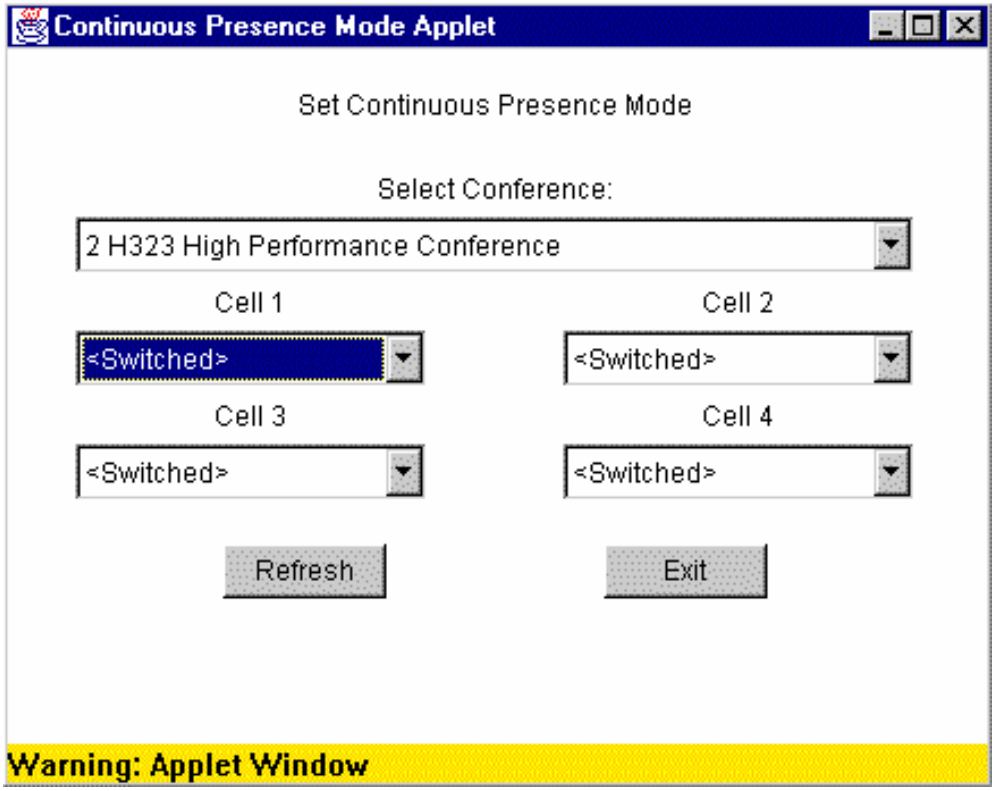
```
http://<yourserver>:8080/cs/cpmode.html
```

where <yourserver> is the IP address or the host name of the computer on which your

Conference Server Conference Administrator Web pages are installed. For example, you could enter the URL using either of the following formats:

```
http://100.11.2.3:8080/radvision/cpmode.html
http://events.radvision.com:8080/cs/cpmode.html
```

The launch page for Conference Server's Continuous Presence Mode applet displays in your Web browser window along with the applet login screen. Enter your Moderator or Administrator user name and password and click **Login**. The Continuous Presence Mode applet displays.



Note:

1. Users can access the Continuous Presence Mode applet through a Start menu shortcut if they install the Conference Server User Tools shortcuts.
2. The Continuous Presence Mode applet can only be used during an active conference.
3. You need to keep the Continuous Presence Mode launch page active while using the applet. However, you can minimize the browser window that displays the page if you choose.
4. If you exit the applet but keep the Continuous Presence Mode applet launch page active in your browser window, you can restart the applet by clicking your browser's Reload (Netscape Navigator) or Refresh (Microsoft Internet Explorer) button.

To define which video will display in each video cell of a continuous presence video stream:

1. Click the Select Conference pull-down menu in the Continuous Presence Mode applet and select the conference for which you want to control the video layout. Only those H.323 continuous presence conferences to which you have been assigned Moderator or Administrator status in the Conference Administrator database will display in the list.

2. The Continuous Presence Mode applet has four pull-down menus representing the four video cells (or quadrants) in a continuous presence video stream. Once you have selected your conference, each pull-down menu displays the list of participants currently connected to your conference. To "pin" a particular participant's video to Cell 1 (top left quadrant of the continuous video stream) click the **Cell 1** pull-down menu and select the participant's name.
3. Repeat Step 2 for **Cell 2**, **Cell 3**, and **Cell 4** as desired. Click the Refresh button at any time to update the list of participants that displays in the Cell pull-down menus.
4. Click Exit to quit the Continuous Presence Mode applet when you are satisfied with the video layout.

Note:

- You can return any individual cell to switched video by selecting **<Switched>** from the appropriate pull down window in the Continuous Presence Mode applet.
- By default, all participants in the conference will receive the continuous presence stream with the video layout you define in the Continuous Presence Mode applet. However, end users have the option of watching individual participant streams instead of the composite continuous presence stream. They can do this by using Conference Server's H.323 VideoSwitcher Applet.

Using Conference Server's H.323 VideoSwitcher Applet

Most H.323 clients today are designed for person-to-person videoconferencing as opposed to group videoconferencing. As a result, H.323 users have no standard way within their client applications to choose which participant to view from among multiple participants in a Conference Server conference. The H.323 VideoSwitcher applet is a Java applet that end users access through a Web browser. It allows H.323 users to participate more fully in a multi-person conference by allowing them to select which participant to view from among multiple connected participants.

Before connecting to Conference Server's H.323 VideoSwitcher applet with your Web browser, you need to be connected to a Conference Server H.323-enabled conference with an H.323 videoconferencing client. Once connected to the conference, launch your Web browser and connect to the following URL:

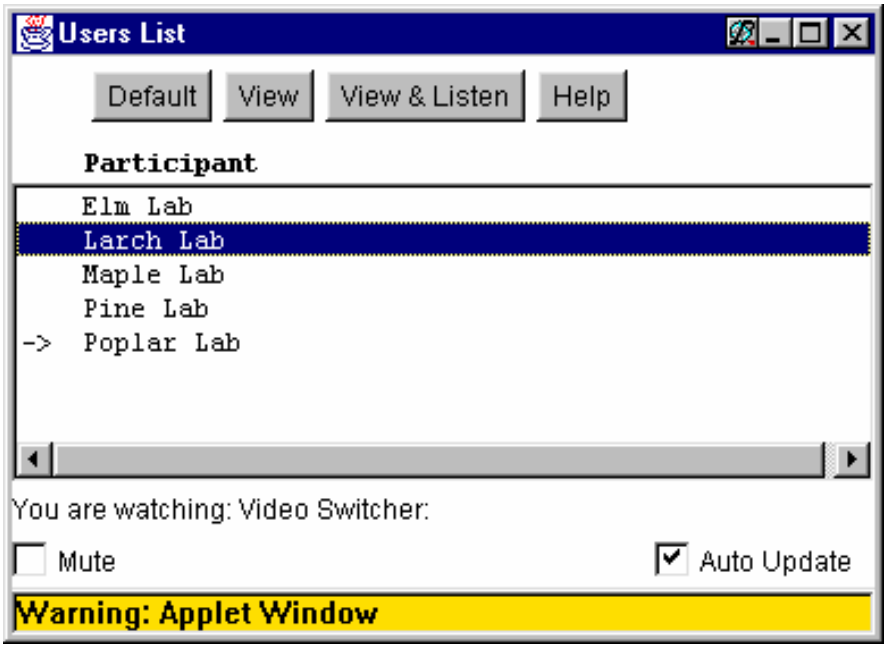
```
http://<yourserver>:8080/cs/h323.html
```

where <yourserver> is the IP address or the host name of the computer on which your Conference Server Conference Administrator Web pages are installed. For example, you could enter the URL using either of the following formats:

```
http://100.11.2.3:8080/cs/h323.html
```

```
http://events.radvision.com:8080/cs/h323.html
```

The launch page for the H.323 VideoSwitcher applet displays in your Web browser window. Click **Start Applet** from the launch page. The H.323 VideoSwitcher applet displays.



The H.323 VideoSwitcher applet is a small applet designed to take up minimal space on an end user's desktop. It consists of the following elements:

Participant

The **Participant** list is a selection box that displays the names of all connected participants. Select a name from the Participant list and then click **View** or **View & Listen** to override default video switching for the conference. Click on the Participant header to sort the list alphabetically.

Default

Select the **Default** button to return video switching to the conference setting. By default, Conference Server switches video based on audio amplitude, but it can also be set to rotate through the video of all connected participants at a timed interval. Clicking the **Default** button will return your video switching to what ever method was set for the conference.

View

Select a name from the Participant list and click the **View** button. The video in your remote window switches to the selected participant but you continue to receive mixed audio from multiple conference participants.

View & Listen

Select a name from the Participant list and click the **View & Listen** button. The video in your remote window switches to the selected participant and you receive audio only from the selected participant rather than mixed audio from multiple conference participants.

Help

Select the **Help** button to view a window with some brief instructions on using the H.323 VideoSwitcher applet.

Mute

Select the **Mute** check box to mute your outgoing audio stream.

Auto Update

Select the **Auto Update** check box to instruct the H.323 VideoSwitcher applet to automatically update its Participant's list every 90 seconds.

The Participant list displays names of connected participants based on user names defined in the client applications. Additionally, it places a small arrow sign (->) in front of the names of participants who have selected your video to view, overriding default video switching for the conference. A status line displays beneath the Participant list indicating the name of the participant whose video you are currently watching.

Note:

- You need to keep the H.323 VideoSwitcher Web page active while using the H.323 VideoSwitcher applet. However, you can minimize the browser window if you choose.
- If you exit the applet but keep the H.323 VideoSwitcher Web page active in your browser window, you can restart the applet by clicking **Show Applet** on the Web page.
- End users can access the H.323 VideoSwitcher applet through a Windows Start menu shortcut if they install the Conference Server User Tools shortcuts.
- In a continuous presence conference, H.323 participants receive a composite video stream of up to four participant videos. However, by using the H.323 VideoSwitcher applet, participants can choose to view individual client streams, or receive switched video rather than the composite video. To view an individual client video, select a name from the Participant list and then click **View** or **View & Listen**. To receive switched video, select "Switched Video" from the Participant list and click **View**. "Switched Video" only displays in the participant list during a continuous presence conference. To return to the continuous presence stream, click **Default**.

Using Conference Server's CallOut applet

Conference Server's CallOut applet is a Java applet that enables Conference Server to initiate conference connections with H.323, T.120, and SIP videoconferencing clients. Users can access the CallOut applet with a Web browser during an active conference or in advance of a scheduled conference and request that Conference Server make a callout to a specific **H.323**, **T.120**, or **SIP** client. If the callout request is made in advance of a scheduled conference, Conference Server adds the request to a call list for the conference and then makes the callout when the conference starts. Videoconferencing clients that receive a request from Conference Server to join a conference will either connect automatically or present a dialog to the user to confirm the connection, depending on how the user has the preference set in his videoconferencing client.

There are no restrictions on who can use the CallOut applet. However, if a conference is password protected, the user must enter the password as part of the callout process.

To access Conference Server's CallOut applet, launch your Web browser and connect to the following URL:

```
http://<yourserver>:8080/cs/callout.html
```

where **<yourserver>** is the IP address or the host name of the computer on which your Conference Server Conference Administrator Web pages are installed. For example, you could enter the URL using either of the following formats:

```
http://100.1.1.1:8080/cs/callout.html
```

```
http://events.radvision.com:8080/cs/callout.html
```

Conference Server's CallOut launch page displays in your Web browser window and

automatically loads the CallOut Java applet.

Note:

End users can access the CallOut applet through a **Start** menu shortcut if they install the Conference Server User Tools application. For more information see Providing Conference Server User Tools to Client End Users.

1. You need to keep the CallOut applet launch page active while using the applet. However, you can minimize the browser window if you choose.
2. If you exit the applet but keep the CallOut applet launch page active in your browser window, you can restart the applet by clicking your browser's **Reload** (Netscape Navigator) or **Refresh** (Microsoft Internet Explorer) button.
3. If you request that Conference Server issue a callout to a client to join a conference that is linked between multiple servers, Conference Server will place the client into *the conference on the server where the user database is located.* You cannot specify which server the client should connect to in a linked conference.

To request that Conference Server initiate a conference connection with an H.323, T.120, or SIP client, follow these steps:

1. Click the **Select Conference** pull-down menu and select an **H.323**, **T.120**, or **SIP** conference from the list. The pull-down menu displays a list of all public conferences in your Conference Server domain. It includes both active and scheduled conferences. It does not display conferences that have been specified as Private or CUSM-only in the conference configuration.
2. If the conference is password protected, the applet displays a conference password dialog. Enter the password for the conference you selected and click **Submit**. The main window of the CallOut applet displays.
3. Select the **protocol** that will be used either **H.323**, **T.120**, or **SIP**.

Note:

- A SIP callout must be made from a SIP enabled conference (not necessary H.323 enabled).
- A T.120 callout can be made from a T.120 enabled conference. This includes H.323 enabled and white board enabled conferences.

4. **Select User(s)**

   Select one or more users. The list of names in the box is derived from user records that have been assigned to the selected conference in the Conference Administrator database. Each user record must specify first and/or last name, IP address, and conference ID in order to display in the Select User(s) box of the CallOut applet. If no user records have been assigned to the conference, the Select User(s) box will be empty.

   The **Enter IP address or alias** field allows you to specify users that do not display in the Select User(s) box. To do this, enter the IP address or alias of the user to whom you want Conference Server to issue a callout. Aliases can be in either of the following two types:

   - **H323-ID**

   An H323-ID alias takes the syntax "NAME:<id>", where <id> is a sequence of alphanumeric characters up to 128 characters in length. For example: NAME:jsmith. H323-ID aliases are used to call H.323 endpoints.

Note: H323-ID aliases apply to H.323, T.120, and SIP callouts.

- **E164**

  An E164 alias takes the syntax "TEL:<number>", where <number> can be any sequence of numeric characters (0-9), number signs (#), asterisks (*), and commas (,) up to 128 characters in length. For example: TEL:5551234. E164 aliases are generally used when calling from a LAN through a gateway to a telephone or other non-H.323 endpoint.

  Use of an alias requires that Conference Server be registered with an H.323 gatekeeper (either its own or a third-party gatekeeper). Conference Server will send the alias to the gatekeeper which will, in turn, resolve the alias to an IP address if possible. If the gatekeeper has no knowledge of the alias the callout cannot be completed.

  Note:

  - E164 aliases only apply to H.323 callouts--not to T.120 or SIP callouts.
  - For information on mapping an H.323 alias to an IP address for Conference Server's internal gatekeeper, see the gk-route command***.***

5. Click **Invite** to submit your call out request to Conference Server. If the conference is active, Conference Server will issue the call out to the H.323 client immediately. If the conference is scheduled for a later time. Conference Server will add the request to its call list for the conference, and issue the callout when the conference begins.
6. When you are finished specifying your callout requests, click **Exit** to quit the applet.

Using Conference Server's MeetingPlanner Applet

Conference Server MeetingPlanner™ is a Java applet that gives end users the ability to create, schedule, edit, and delete Conference Server conferences. The conferences that an end user creates with the applet are based on template conferences that have been created in advance by an administrator. MeetingPlanner de-centralizes the conference creation process, extending it to the end user while leaving ultimate control over network resources in the hands of the administrator.

The MeetingPlanner applet is designed as a tool to help service providers roll out large-scale videoconferencing services without the need to hire human operators to configure conferences for customers. It can also be used by other organizations that would like to give certain users the ability to create conferences on their own, without giving them access to Conference Server's more powerful Conference Administrator Web pages. A busy system administrator may set up one or more Conference Servers on the company LAN, configure template conferences for his users, and allow the users to schedule their own conferences

Note: The MeetingPlanner applet can be used to create only single server conferences. It cannot be used to create linked conferences.

There are several steps you must take as an administrator before an end user can use the MeetingPlanner applet. These are:

1. Create a template conference.
2. Create an 'Organization' and assign it a template conference.
3. Create a user record and assign it to an organization.

4. Define your e-mail server.

The following sections explain these steps in more detail.

Create a Template Conference

The first step you must take to enable an end user to create conferences with Conference Server's MeetingPlanner applet is to create a template conference. A template conference allows you to define a set of rules that will apply to the conferences end users create with the MeetingPlanner applet. This allows you to control the parameters of conferences, ensuring the integrity of your network resources, while allowing end users the freedom to create their own conferences (when they need them and without requiring your help!).

You can create as many different template conferences as you need. For example, if you are a service provider, one of your customers might be a local business that conducts daily sales meetings over the Internet with its offsite sales representatives. This customer needs a template for small, private, interactive conferences hosted on a single Conference Server. Another customer could be a local radio station that broadcasts a weekly concert series over the Internet. This customer requires a template for a one-way cybercast to multiple Conference Servers.

To create a template conference, navigate to the Conferences area of Conference Server's Conference Administrator Web pages and click **Add H.323** or **Add CUSM**. The **Add H.323** or **Add CUSM** page displays. Proceed to create the conference as you would any other Conference Server conference (see Adding a Conference). To designate the conference as a template conference, select the check box labeled **This conference is a template** under the Template section on the Add Conference page. Additionally, you can enter a text message in the **Template Description** text box. The description you enter will display in the MeetingPlanner applet and should help users make informed decisions about which templates to choose for the conferences they create.

Note: When creating a conference template. Double quotes (") is not an allowable character to be used when entering a template description.

By creating a template conference, you can define the following parameters for the conferences that end users create with the MeetingPlanner applet:

- Conference Attributes: Video, Audio, Chat, H.323 w/T.120, SIP, People + Content
- Broadcast Mode
- Maximum Participants
- Reject Messages for Conference Full, Authentication, and Invalid Password
- Conference Duration (for General Users only; Conference Managers can set duration)
- Multicast Attribute and Address Information
- Maximum Send and Receive Rates
- Connection Time Limits

- Data Collaboration for CUseeMe protocol users
- RADIUS Billing and Authentication
- Preferred/required Audio and Video Codecs
- Audio Latency
- Tracking, Self Reflect, and Root Modes
- Conference Server Layout

For a complete description of these parameters, see Adding a Conference

Note: A template conference is not enabled for videoconferencing use. It is used solely as a model on which to base other conferences.

Create an Organization Record

After you have created one or more template conferences, you need to create an 'organization' record. An organization record provides a way to associate users with template conferences. For example, if you are a network administrator for a large corporation you might create several different organization records, such as 'Marketing', 'Sales', 'Engineering', and so on. The members of each organization have a set of requirements for the conferences in which they participate. They also have one or more representatives that will access the MeetingPlanner applet to create those conferences. When you create an organization record, you assign it one or more template conferences. Later you create user records for those users that will access the MeetingPlanner applet. You associate each user record with an organization record. A user that accesses Conference Server's MeetingPlanner can create conferences with the templates you have assigned that user's organization.

To create an organization record, navigate to the Users area of Conference Server's Conference Administrator Web pages and click **Organizations** . For step-by-step instructions see Managing Organizations.

Create a Conference Manager User Record

After you have defined your template conferences and organization records, you need to create user records for those people that will access the Conference Server MeetingPlanner applet. To create a user record, navigate to the Users area of Conference Server's Conference Administrator Web pages and click **Add**. The **Add User** page displays. At a minimum, you must provide the following information in the user record:

- Username
- Password
- User Permission (Conference Manager or General User/Normal)
- Organization

Note: If you intend to allow a user to send e-mail invitations for the videoconferences (s)he creates, you must also enter the that user's e-mail address in the user record. This serves as the return address (Reply-to field) on the e-mail invitation.

The type of permission you assign a user depends on the level of control you want that user to have over the conferences (s)he creates. The most

important differences between conference managers and general users can be summarized as follows:

- Conference managers can create, edit, and remove scheduled conferences (specifying start date, start time, conference duration, and repeat interval); general users can create temporary conferences "on-the-fly", which start at the time of creation and are deleted after a conference duration determined by the template conference.
- Conference managers can create conferences that require username/password authentication, and create user records to specify which participants are allowed to connect; general users are limited to creating unauthenticated conferences, or conferences that require a conference password only.

Table: Conference Manager Versus General Users

Conference Control	General User (MeetingPlanner Applet)	Conference Manager (MeetingPlanner Applet)
Create a Scheduled Conference (specify start date, start time, conference duration and repeat interval)	NO	YES
Create a Temporary Conference	YES	YES (Never repeat option)
Edit a Conference	NO	YES
Remove a Conference	NO	YES
Specify Conference Name	YES	YES
Specify Conference Greeting	YES	YES
Specify Conference Password	YES	YES
Limit Maximum Participants	NO	YES (up to number specified by the Template)
Specify Conference Authentication	YES	YES
Limit Conference to Specific Participants	NO	YES
Create and Edit User Records	NO	YES
Send E-mail Invitations	YES	YES

Distribute to your end users the user names and passwords you have defined for them in their user records. These are used to log in to the Conference Server MeetingPlanner applet.

MeetingPlanner

To access the Conference Server MeetingPlanner applet, launch your Web browser and connect to the following URL:

```
http://<yourserver>:8080/cs/planner.html
```

Note that <yourserver> is the IP address or the hostname of the computer on which your Conference Administrator Web pages are located. For example, you can enter the URL using either of the following formats:

```
http://100.11.2.3:8080/cs/planner.html
```

```
http://events.radvision.com:8080/cs/planner.html
```

The MeetingPlanner launch page displays in your Web browser window. When you access this launch page, the MeetingPlanner Java applet automatically loads and displays a login screen.

In order to use the MeetingPlanner applet, your Conference Server administrator must create a user record for you in the Conference Administrator database. The administrator must assign you either Conference Manager or General User permission (see **Assigning special permissions**). Once you enter your username and password, the MeetingPlanner applet presents a different set of screens depending on whether you login as a conference manager or general user.

Note:

- You need to keep the MeetingPlanner launch page active while using the MeetingPlanner Java applet. You can minimize the browser window if you choose.
- If you exit the applet but keep the MeetingPlanner launch page active in your browser window, you can restart the applet by clicking **Restart** on the launch page.

Using MeetingPlanner with General User permission

As a user assigned General User status for an organization, you can create temporary conferences "on-the-fly" with the MeetingPlanner applet. Temporary conferences are available immediately after you create them and are removed automatically and immediately after completion. Your Conference Server administrator specifies in the conference template how long a conference can last.

To create a conference:

1. Access the MeetingPlanner Web page (see **Accessing MeetingPlanner**). The MeetingPlanner Java applet loads.
2. Enter your username and password in the MeetingPlanner login screen. Click **Login**.

   Note: Your Conference Server administrator can provide you with a username and password for the MeetingPlanner applet.
3. Enter a name for your conference in the Conference Name field. You can also add an optional text message in the Conference Greeting field. This message will display to CUseeMe protocol users when they first connect to the conference. H.323 client users will **not** see this message. The Conference Greeting is limited to 918 characters.

   Click **Next** to continue.
4. Select a template for your conference from the **Template** pull-down menu. Your Conference Server administrator creates templates in advance and assigns them to your organization. You may see only a single or several template choices in this list. Each template includes a description so that users can distinguish its characteristics. When you select a template in the MeetingPlanner applet, this description displays in the Template description text box.

   Note: You can use the MeetingPlanner to create single server conferences only. You cannot use it to create linked conferences.

   Click **Next** to continue.

5. Select a security option for your conference. You can choose from:

   - *This conference is open to everyone* - The Conference Server does not authenticate users for this conference. It will be open to participants on a first come, first served basis.
   - *This conference is password protected* - Users must enter a password to connect to the conference. CUseeMe-protocol client and NetMeeting users can specify a conference password within their client applications. Other H.323 users must use the User Authentication Web page to enter a conference password before connecting with videoconferencing clients.

   Click **Next** to continue. The subsequent screens depend on the security option you chose for your conference. The remaining steps for each option follow (each begins with a step number 6):

Option: This conference is open to everyone

6. In the **E-mail** field, enter an email address to which you want to send an invitation. Click **Add New**. The MeetingPlanner adds the email address to the Invited Users list. Repeat this step for each person you want to invite (up to the maximum number of participants allowed in the conference).

   Click **Next** to continue.

   Note: If your Conference Server administrator did not define an email server for outgoing messages, this screen and the screen described in the following step do not display. The MeetingPlanner applet instead skips to the final screen.

7. The MeetingPlanner displays the default invitation message to the email addresses you entered. You can review the message and modify it in the text box.

   Note: The Meeting Planner sends email invitations only once, even for scheduled or repeat conferences. The MeetingPlanner sends the email invitation when you create the conference.

   Click **Next** to continue.

8. The MeetingPlanner displays a screen with a list of the settings you can chose for your conference. If you want to change a setting, click **Back** until you reach the screen that you want. When you are satisfied with the settings, click **Finish**. The MeetingPlanner creates your conference and closes the applet. It then launches the User Authentication Web page.

   If you are connecting with an H.323 client, select the check box labeled **I am using an H.323-compatible client** on the User Authentication Web page. Click **Authenticate**. The Conference Server displays a Web page with the IP address of the server hosting your videoconference. Close the User Authentication Web page and connect to the specified server with your videoconferencing client.

Option: This conference is password protected

7. In the **Password** field, enter a password for your conference. Enter it again in the **Verify** field. To include the password in the email invitation for the conference, select **Append password to the URL of outgoing e-mails**.

   Click **Next** to continue.

8. In the E-mail field, enter an email address to which you want to send an invitation. Click Add New. The MeetingPlanner adds the email address to the Invited Users list. Repeat this step for each person you want to invite (up to the maximum number of participants allowed in the conference).

Click **Next** to continue.

Note: If your Conference Server administrator did not define an email server for outgoing messages, this screen and the screen described in the following step do not display. The MeetingPlanner applet instead skips to the final screen.

9. The MeetingPlanner displays the default invitation message to the email addresses you entered. You can review the message and modify it in the text box.

   Note: The Meeting Planner sends email invitations only once, even for scheduled or repeat conferences. The MeetingPlanner sends the email invitation when you create the conference.

   Click **Next** to continue.

10. The MeetingPlanner displays a screen with a list of the settings you can chose for your conference. If you want to change a setting, click **Back** until you reach the screen that you want. When you are satisfied with the settings, click **Finish**. The MeetingPlanner creates your conference and closes the applet. It then launches the User Authentication Web page.

    In the text field labeled **Specify Conference Password (if required)** on the User Authentication Web page, enter the password for the conference. If you are connecting with an H.323 client, you also must select **I am using an H.323-compatible client**. Click **Authenticate**.

    The Conference Server displays a Web page with the IP address of the server hosting your videoconference. Close the User Authentication Web page and connect to the specified server with your videoconferencing client.

Using MeetingPlanner with Conference Manager permission

When you log in to the MeetingPlanner applet as a conference manager, the applet displays a screen with a conference selection box and buttons to add, edit, or remove a conference.

To create a conference, follow these steps:

1. Access Conference Server MeetingPlanner Web page. The MeetingPlanner Java applet loads.
2. Enter your username and password in the MeetingPlanner log in screen, and click **Login**.

   Note: Your Conference Server administrator can provide you with a username and password for the MeetingPlanner applet.

   MeetingPlanner displays a screen with a conference list showing Conference Name, Conference ID and the following buttons: Add Conference, Edit Conference, Remove Conference, Refresh List, and Exit.

   The conference selection box displays a list of all the conferences that have been created by users assigned to your organization by your Conference Server administrator. If you are the first user from your organization to access the MeetingPlanner applet, the conference selection box will be empty.

3. Click **Add Conference**. The Add Conference wizard displays.
4. Enter a name for your conference in the **Conference Name** field. You can also add an optional text message in the Conference Greeting field. This message will display to users when they first connect to the conference. H.323 users will not see this message. The Conference Greeting is limited to 918 characters.

   Click **Next >** to continue.

5. Select a template for your conference from the **Template** pull-down menu. These

templates have been created in advance by your Conference Server administrator and assigned to your organization. You may see only a single template choice in this list or several. When your administrator creates a conference template, (s)he can include a description of the template so that users can distinguish the characteristics of each. When you select a template in the MeetingPlanner applet, this description displays in the Template description text box.

Note: The MeetingPlanner can be used to create only single server conferences. It cannot create linked conferences.

Click **Next >** to continue.

6. Enter scheduling information for your conference including start date, start time, duration of conference, and repeat interval.

    - **Start Date -**Specifies the month, day, and year that Conference Server will start your scheduled conference. A scheduled conference is dormant (disabled) until five minutes before the date and time specified by the Start Date and Start Time fields.
    - **Start Time -** Specifies what time Conference Server will start your scheduled conference. You should enter the Start Time for a conference in the local time of the computer system to which your browser is connected (using the twelve hour A.M./ P.M. notation). Conference Server will translate the local time, based on that computer's system clock, to the Universal Time Coordinated (UTC), formerly called Greenwich Mean Time (GMT). UTC is a world standard consisting of 24 time zones. By translating the time to UTC, Conference Server will start the conference at the correct time on every server hosting the conference -- even if those servers are located in several different time zones.
    - **Duration -** Specifies how long a scheduled conference will last. You specify the duration in hours and minutes, with a minimum duration of 1 hour (1:00) and a maximum duration of 24 hours (24:00). When the duration of a conference is complete, Conference Server automatically disables the conference and disconnects any remaining participants. If you select Never as your repeat option, Conference Server will delete the conference after the specified duration.
    - **Repeat Conference -** Specifies whether Conference Server will automatically repeat a scheduled conference daily, weekly, monthly, or never (the default is **Never**). Conference Server adjusts the start date of the conference by the required interval after each occurrence of the conference, and enables the conference again at the specified interval. If you select **Never**, Conference Server deletes the conference.

    The **Monthly** repeat option repeats a conference on the same day of a particular week in subsequent months. For example, if you specify August 1, 2000 (first Tuesday of August) as the start date of a conference with a monthly repeat option, Conference Server will repeat the conference on September 5, 2000 (first Tuesday of September), October 3, 2000 (first Tuesday of October), and so on. If you specify a day during the fifth week of a month as the start date, Conference Server will repeat the conference on that day in the last week of subsequent months. For example, if your starting date is August 30, 2000 (fifth Wednesday of August), Conference Server will repeat the conference on September 27, 2000 (fourth and last Wednesday of September), October 25, 2000 (fourth and last Wednesday of October), November 29, 2000 (fifth and last Wednesday of November) and so on.

    Click **Next >** to continue.

7. Select the number of participants you will allow in the conference. The maximum number you can select was set by the your Conference Server administrator in the conference

template. While you can decrease the maximum number of participants, you cannot increase or exceed the administrator's limit.

Click **Next >** to continue.

8. Select a security option for your conference:

   - This conference is open to everyone - Conference Server will not try to authenticate users for this conference. It will be open to participants on a first come, first serve basis.
   - This conference is password protected - Users need to enter a password to connect to the conference. CUseeMe protocol and NetMeeting users can specify a conference password within their client applications. Other H.323 users need to use Conference Server's User Authentication Web page to enter a conference password before connecting to the conference with their videoconferencing clients.
   - This conference is limited to specific participants - Only those participants whom you define will be able to access the conference. These participants need to use Conference Server's User Authentication Web page to enter a personal username/password combination before connecting to the conference with their videoconferencing clients.

   Click **Next >** to continue. The screens that display next depend on the security option you chose for your conference. The remaining steps for each option follow:

Option: "This conference is open to everyone"

9. A screen displays that allows you to define addresses to which MeetingPlanner will send e-mail invitations for the videoconference. In the **E-mail** field, enter the e-mail address of a person to which you would like to send an invitation, and click **Add New**. MeetingPlanner adds the e-mail address to the Invited Users list. Repeat this step for each person you want to invite (up to the maximum number of participants allowed in the conference).

   Click **Next >** to continue.

   Note: If your Conference Server administrator did not define an e-mail server for outgoing messages, this screen and the screen described in the following step will not display. The MeetingPlanner applet will take you instead to the final screen described in Step 11.

10. MeetingPlanner displays the default invitation message that will be sent to the e-mail addresses you specified in the previous step. Review the message and modify it in the text box as desired.

    Note: MeetingPlanner e-mail notification is sent only ONCE, even for scheduled or repeat conferences. The e-mail is sent at the time of conference creation.

    Click **Next >** to continue.

11. MeetingPlanner displays a screen with a list of the settings you chose for your conference. Check to see that these settings are correct. If you want to change a setting, click **< Back** until you reach the appropriate screen. If you are satisfied with the settings, click **Finish**. MeetingPlanner will create your conference. Participants will not be able to enter the conference until five minutes before the scheduled start time.

Option: "This conference is password protected"

9. Enter a password for your conference in the **Password** field. Make sure that you have entered the password correctly by entering it again in the **Verify** field. If you would like to include the password in the e-mail invitations MeetingPlanner sends out for the

conference, select the check box labeled **Append password to the URL of outgoing e-mails**.

Click **Next >** to continue.

10. A screen displays that allows you to define addresses to which MeetingPlanner will send e-mail invitations for the videoconference. In the **E-mail** field, enter the e-mail address of a person to which you would like to send an invitation, and click **Add New**. MeetingPlanner adds the e-mail address to the Invited Users list. Repeat this step for each person you want to invite (up to the maximum number of participants allowed in the conference).

    Click **Next >** to continue.

    Note: If your Conference Server administrator did not define an e-mail server for outgoing messages, this screen and the screen described in the following step will not display. The MeetingPlanner applet will take you instead to the final screen described in Step 12.

11. MeetingPlanner displays the default invitation message that will be sent to the e-mail addresses you specified in the previous step. Review the message and modify it in the text box as desired.

    Note: MeetingPlanner e-mail notification is sent only ONCE, even for scheduled or repeat conferences. The e-mail is sent at the time of conference creation.

    Click **Next >** to continue.

12. MeetingPlanner displays a screen with a list of the settings you chose for your conference. Check to see that these settings are correct. If you want to change a setting, click **< Back** to go to the appropriate screen. If you are satisfied with the settings, click **Finish**. MeetingPlanner will create your conference. Participants will not be able to enter the conference until five minutes before the scheduled start time.

Option: "This conference is limited to specific participants"

9. MeetingPlanner displays a screen with two selection boxes: **Available Participants** and **Invited Participants** . The Available Participants box lists the names of any users previously defined for your organization. These include:

10. Users that your Conference Server administrator assigned General User status and associated with your organization by creating a user record in Conference Server's Conference Administrator database.

11. Users that you, and other conference managers from your organization, have defined in the MeetingPlanner applet for other conferences.

    Click **Add New** to define a new user that you would like to include as a participant in your videoconference. For each new user you must enter the following information and click **OK** in the Add User screen:

    User Name

    Accepts a maximum of 32 characters.

    Password

    Accepts a maximum of 15 characters.

    Last Name

    Accepts a maximum of 35 characters.

    First Name

Accepts a maximum of 35 characters.

E-mail

Accepts a maximum of 50 characters.

Note: The user identifier fields do not accept the following characters: double-quote ("), single quote ('), back slash (\ ), forward slash (/), semi-colon (;), asterisk (*), question mark (?), and percent sign (%). Additionally, the Username and Password fields do not accept spaces.

The username for each user you define appears in the Available Participants list. Select a user from the Available Participants list and click **Invite >>**. MeetingPlanner will move the name from the Available Participants list to the Invited Participants list. Repeat this step for each user you want to attend your videoconference. If you want MeetingPlanner to send out e-mail invitations for the conference to the intended participants, select the check box labeled **e-mail Invitation**.

Note:

- If your Conference Server administrator did not define an e-mail server for outgoing messages, the check box labeled "E-mail Invitation" will be hidden and the screen described in the following step will not display. The MeetingPlanner applet will take you instead to the final screen described in Step 11.
- If you click a user name in the Available Participants or Invited Participants lists, the following information for that user will display in the Participant Info box: last name, first name, and e-mail address. This is for information purposes only -- you cannot edit this text. If you want to edit user information, select the user name and click **Edit**.

  Click **Next >** to continue.

9. MeetingPlanner displays the default invitation message that will be sent to the participants you specified in the previous step. Review the message and modify it in the text box as desired.

   Note: MeetingPlanner e-mail notification is sent only ONCE, even for scheduled or repeat conferences. The e-mail is sent at the time of conference creation.

   Click **Next >** to continue.

10. MeetingPlanner displays a screen with a list of the settings you chose for your conference. Check to see that these settings are correct. If you want to change a setting, click < Back to go to the appropriate screen. If you are satisfied with the settings, click Finish. MeetingPlanner will create your conference. Participants can begin to enter the conference five minutes before the scheduled start time.

    Note: If you click **Finish** on any of the applet screens before reaching the final screen, MeetingPlanner jumps you to the final screen where you need to click **Finish** again. MeetingPlanner will create the conference based on default settings for any of the screens you did not complete.

    In addition to adding new conferences, you can edit and remove existing ones for your organization. To do this, log in to the Conference Server MeetingPlanner applet as a conference manager. In the conference selection box that displays, click on the conference you want to edit or remove. Click **Edit Conference** or **Remove Conference**. The Edit Conference process presents the same set of screens that you see when you add a conference. Make edits as necessary and click **Finish** to submit your edits.

Providing Conference Server User Tools to client end users

Conference Server User Tools is a simple application that installs Start menu shortcuts to Conference Server's MeetingPlanner applet, User Authentication Web (Login) page, CallOut applet, and Continuous Presence Mode applet. It is a Microsoft Windows-based executable that you can distribute to videoconferencing client end users in your organization.

You can find the Conference Server User Tools installer in the UserTools directory of your Conference Server CD-ROM. Distribute this file, called **Conference Server User Tools.msi**, to your client end users and provide them with the following installation information:

- IP address of the third-party HTTP server that manages Conference Server's Conference Administrator Web pages. If you have more than one installation of the Conference Administrator Web pages for your domain, you can balance the load between the various installations if you choose.
- Port number that your third-party HTTP server uses to manage Conference Server's Conference Administrator Web pages.

Historical statistics

Conference Server enables you to log to a file the summary statistics concerning activity on your server. The following fields on the **Add Domain Member** page govern how Conference Server logs this information.

Log file name

The **Log file name** field specifies a name and directory path for the log file to which Conference Server will write summary statistics for the Conference Server. By default, Conference Server names the log file **cs.stats** and writes it to the Conference Server installation directory. If you change the name you should keep the .stats extension. When Conference Server creates a backup of the log file, it inserts a date/time stamp between the main part of the file name and the .stats extension.

Log interval

The **Write to log every** field specifies at what interval (in seconds) Conference Server will write summary statistics to the log file. By default, Conference Server sets this interval to 600 seconds (10 minutes). Each time data is written to the file, Conference Server includes a date/time stamp. You should be careful not to set too frequent a time interval. Log files can become large very quickly and require frequent backup. In addition, gathering statistics is a CPU intensive operation and can slow the performance of your Conference Server.

Note: You must specify an integer greater than 0 (zero) in the **Write to log every** field, if you want Conference Server to generate statistics for your server. This impacts real-time statistics as well as historical statistics. Real-time statistics are accessible from the Monitoring area. If you want real-time statistics but do not want to generate a stats log file, enter a value greater than 0 (zero) in the **Write to log every** field, and enter 0 (zero) in the **Max number of lines** field.

Line limit

The **Max number of lines** field determines whether Conference Server will create a stats log file and defines how large Conference Server will allow that file to get before creating a backup. The size of the file is specified in number of lines. By default, Conference Server sets this field to 0 (zero). A zero value prevents Conference Server from creating a stats log file. To enable Conference Server to create a stats log file, enter a positive integer greater than 0 (zero) in the **Max number of lines** field. A suggested line limit is 10000 lines.

Note: If you want Conference Server to create a stats log file but do not want to base backups on the number of lines in the file, enter -1 in **Max number of lines** field. This instructs Conference Server to create a stats log file, but to backup the file at the interval specified in the **Backup every** field.

Backup interval

The **Backup every** field specifies at what interval (in days) Conference Server will backup the stats log file. Once a backup is created, Conference Server clears the original log file of all data and begins writing new data to it. If you enter a positive integer greater than 0 (zero) in the **Backup every** field, Conference Server will perform a backup whenever the Conference Server (re)starts, and repeatedly at the interval specified. If you enter 0 (zero) in the **Backup every** field, Conference Server will use the **Max number of lines** field to determine when backups are done.

Note: Backup stats files are never purged. They are left in the product installation directory (or in the directory specified in the **Log file name** field) for the administrator to use as needed and delete as desired.

Interfacing with Third-Party Billing Systems

Demand for multimedia group interaction is strong and growing. Consumer end users want to participate in interactive cybercasts and videochat. Business participants want to collaborate without having to spend time and money traveling to common physical locations. In order to meet this growing demand, service providers and other organizations are adding multipoint videoconferencing to their menu of available services. Conference Server provides the ability to interface with third-party billing systems, enabling service providers and other businesses to offer multipoint videoconferencing services for a fee.

Many large service providers already have sophisticated systems in place to bill for services. Conference Server does not replace these systems, but rather is capable (with some customizing) of feeding them the necessary data for the billing of metered videoconferencing services.

For more information, see the next section, “Understanding Conference Server’s Billing Architecture.”

Understanding Conference Server's Billing Architecture

Different organizations use different systems to authenticate, track, and bill their customers for services. RADVISION designed Conference Server with the flexibility to accommodate these varying systems. The Conference Server architecture includes an “abstraction layer” that exists between the core Conference Server application and customized billing modules. The abstraction layer specifies the type and format of data that Conference Server sends for billing/authentication purposes. The billing modules provide the communication interface between Conference Server and third-party billing/authentication systems.

Vendor-specific billing modules can be written and plugged in to the Conference Server abstraction layer. Currently, Conference Server provides a billing and authentication module for servers that use the RADIUS (Remote Authentication Dial-In Service) protocol. Several different vendors provide RADIUS billing and authentication servers.

Conference Server's RADIUS billing module includes a RADIUS client application. The RADIUS client communicates with your RADIUS server by sending authentication and accounting requests. Authentication request packets contain the username and password that a user enters through Conference Server's User Authentication Web page and a "shared-secret" that identifies Conference Server's RADIUS client to the RADIUS server. The RADIUS server receives the request, verifies the user in its users file, and sends an

acceptance packet back to Conference Server's RADIUS client. Conference Server then issues a one-time-admit privilege to the user's client for the specified conference.

Accounting request packets contain user connection statistics, also called session data, that your RADIUS server uses for accounting/billing purposes. An Accounting Start packet is sent when a user connects to your Conference Server, and an Accounting Stop packet is sent when the client disconnects.

Note: A single RADIUS server is configured to serve your domain of Conference Servers. However, you can specify on a per-conference basis whether or not you want RADIUS billing and/or authentication enabled. See Defining your RADIUS server and User authentication.

Session Data

During conference configuration, you can choose to have Conference Server forward end user session data to your third-party billing/authentication system. Session data is specific information about each end user videoconferencing session. It consists of the following:

- Conference ID
- Client IP address
- Username
- Password
- Start Time
- Elapsed Time
- Stop Time
- Stop Reason
- Total bytes sent
- T.120 bytes sent

Your third-party billing system will need this session data if you intend to charge customers for *metered* videoconferencing services. However, it may not be necessary to forward this information if you charge customers a flat fee for videoconferencing services and want only to authenticate users through your third-party system.

Conference Server creates a series of files at startup to capture client session data in the event of disruptions of service. These files create a snapshot of the state of your Conference Server. When you enable billing, Conference Server sends session data to your third-party billing system each time a client disconnects. However, if service is unexpectedly disrupted, the following files prevent loss of session data:

cs.cur

Saves current time every minute

cs.sdf

Lists currently connected clients

***.sdf**

Client session data files (where * is the client IP address)

When you restart Conference Server after a disruption, it will reference these files and send the appropriate session data to your third-party billing system. Conference Server continually writes current information to these files and deletes information as it becomes obsolete. In this way, the files always reflect the current state of your Conference Server and do not ever

need to be purged.

User Authentication

If you choose to authenticate and/or bill users through a third-party system, your users will first need to connect with a browser to Conference Server's User Authentication Web page. From the User Authentication Web page, a user can submit an authentication request to join a conference. Then the Conference Server queries the third-party system for user authentication. The Conference Server only allow users authenticated by the third-party system to connect to the requested conference.

Defining Your RADIUS Server

From the **Define RADIUS Server** page, you can specify the parameters that Conference Server's RADIUS (Remote Authentication Dial-In User Service) client will use to communicate with your third-party RADIUS server. The settings on the Define RADIUS Server page enable RADIUS billing and authentication for your entire Conference Server domain. However, you can decide on a per conference basis, whether or not to use RADIUS for billing and/or authentication purposes.

To define communication parameters for the third-party RADIUS server for your Conference Server domain:

1. Click the **Network** button on the Conference Server entry page or click the **Network** icon that displays in the main navigation bar. The **Network** page displays.
2. Click the **RADIUS** button on the Network page. The **Define RADIUS Server** page displays.
3. Select the **Enable RADIUS** check box to enable communication between Conference Server's RADIUS client and your third-party RADIUS server. When you submit this page with the "Enable Radius" check box selected, Conference Server's RADIUS client can send authentication and accounting requests to your RADIUS server and receive responses in return. When you submit this page with the check box cleared, communication between Conference Server's RADIUS client and your RADIUS server stops.
4. In the field labeled **RADIUS Server IP Address,** enter the location of your third-party RADIUS billing and authentication server. The location is specified using the server's IP address in standard dot notation.
5. In the field labeled **RADIUS Server Port**, enter the UDP (User Datagram Protocol) port over which Conference Server's RADIUS client sends authentication requests to your RADIUS server. The RADIUS protocol defines the UDP authentication port as 1812, but some older RADIUS server implementations use port 1645. Conference Server defaults to port 1812.
6. In the field labeled **RADIUS Accounting Port**, enter the UDP port over which Conference Server's RADIUS client sends accounting requests to your RADIUS server. The RADIUS protocol defines the UDP port used for accounting requests as 1813, but some older RADIUS server implementations use port 1646. Conference Server defaults to port 1812.
7. In the filed labeled **Retry Limit**, specify the number of times Conference Server's RADIUS client will re-send an authentication or accounting request if it receives no response from your RADIUS server. The RADIUS protocol uses UDP as its transport protocol. UDP does not guarantee that packets will be delivered from sender to receiver. If Conference Server's RADIUS client sends a packet to your RADIUS server but does not receive a response, it will repeatedly send the packet again until it receives a

response from the server or reaches its retry limit.

8. In the field labeled **RADIUS Shared Secret**, enter an authentication password that Conference Server's RADIUS client will use to communicate with your RADIUS server. The authentication password is known as a "shared secret" between RADIUS client and RADIUS server. Shared-secrets are case-sensitive and have a maximum length of 15 alphanumeric characters. The shared-secret you enter must match the corresponding shared-secret in the clients file of your RADIUS server.
9. In the field labeled **RADIUS Shared Secret Confirm**, re-enter the authentication password you just entered in the RADIUS Shared Secret field. This is to confirm that you entered the password as intended.
10. Click **Submit**.

Enabling Streaming Media

Streaming Media is an add-on option you can purchase for your Conference Server. The option enables you to route audio and video from a Conference Server H.323 conference to a third-party streaming media encoder, which in turn allows you to distribute the stream live or on demand from a third-party streaming media server. Conference Server's Streaming Media option provides you the ability to integrate two-way interactive videoconferences with streaming media distribution technology. For example, you may have an interactive videoconference between four participants. You could configure the conference in continuous presence mode so that Conference Server would create a composite video stream of the four participants. Conference Server would perform audio mixing of the H.323 audio streams. You could then send the audio and video streams out to a streaming media encoder/server so that large numbers of people could view and listen to the interaction between the four conference participants.

Enable the Streaming of a Conference Server Conference

You need to issue the Telnet command **stream-media** OR use the Conference Server GUI to enable the streaming AFTER you have the following in place:

A Conference Server Conference Server with the Streaming Media add-on option installed.

An H.323 conference configured on your Conference Server,

specifying G.711 (A-law or μ-Law), G.723.1, or G.729A as the required audio codec and one of the following as the required video codec:

- H261.CP4
- H261.CIF
- H261.QCIF
- H263.CIF
- H263.QCIF
- H263.SQCIF

Note: The H261.CP4 video codec enables continuous presence for your conference, provided that you have Conference Server's Continuous Presence option installed. In an H.323 continuous presence conference, Conference Server routes a composite video stream with the videos of up to four conference participants. In a standard H.323 conference, Conference Server routes video based on default video switching for the conference. In both cases, Conference Server performs audio mixing of the H.323 audio streams.

A Windows 2000 system with Conference Server's streaming media audio and video capture drivers installed.

Third-party streaming encoder/exporter software should also be installed on this system. The installer for Conference Server's streaming media audio and video drivers is included on the Conference Server CD in a directory called StreamMedia.

You have the following options during installation:

Complete Setup: This option installs the drivers using the default ports for audio and video and the appropriate test tool at the default location **Program Files\CLICK TO MEET\Stream Media**.

Custom Setup: This option gives the user the opportunity to change the ports for audio and video and to specify an alternative installation location for the appropriate test tool.

If you install on Windows NT, the tool "capture.exe" will be installed, utilizing Video For Windows technology. If installing on Windows 2000, the tool "streamview.exe" will be installed, utilizing DirectX technology.

Additional Information on Installing Conference Server's Streaming Drivers

You need to specify the "Stream Audio" and "Stream Video" drivers as input sources in the streaming media encoder application. Some encoders, such as Microsoft Windows Media Encoder, allow you to specify alternative input sources. Other encoders may require that you change the registry settings to specify the Conference Server drivers as default input sources.

You need to set up the necessary streaming parameters within the encoder application. Use the appropriate video image size to match the Conference Server video codec you are using in the conference. To do this, set the video driver format option to use either **CIF** (352 x 288 pixels) or **QCIF** (176 x 144 pixels), and set the color space to **IYUV**. Conference Server's audio driver uses **8000 samples/second** and **16-bits/sample** wave format. In most cases, the Windows multimedia subsystem will query the driver for the correct format so you don't need to specify these settings. Specify appropriate bandwidth for your network if you intend to broadcast. Set the file name if you want the encoder to record.

For specific instructions on installing and using your third-party streaming encoder/exporter software, consult the documentation that came with the product(s).

Now issue the stream-media command

After all your software components are properly configured and at least one H.323 videoconferencing client is connected to your H.323 conference, establish a Telnet connection to your Conference Server. Enter the stream-media command as follows:

```
stream-media -c <id> enable <IP address>
```

where <id> is the conference number of the H.323 conference you want to stream, and <IP address> is the IP address of the system on which the Conference Server audio and video drivers are installed. By default, the stream-media command uses UDP port 1424 to route audio and 1414 to route video. In most cases, these port numbers do not need to be changed. However, the stream-media command does accept optional video and audio port numbers that you can use to override Conference Server defaults if you experience a port conflict. For more information on using the stream-media Telnet command, see the stream-media command.

When you enable the stream-media command, Conference Server attempts to connect to the IP address specified in the command and route the live conference media streams to the audio and video drivers. These drivers function like true audio record and video capture drivers. They receive audio/video from Conference Server, decode it, and forward it to the streaming media encoding application when requested.

Display a message before Conference Server sends video

The streaming video driver can display a pre-connection message. It requires low bandwidth and can be useful for the following:

- An indication that there is no video data reaching the driver
- A way to pass relevant information to the viewers: for example, you can send messages such as, "Company quarterly meeting", or "Staff meeting will start at 11:00am EST".
- A way to set up streaming before the conference starts without depending on the conference clients and server: depending on what application you choose, streaming setup may take some time. You may want to send a message before the conference data is available. When you see the message displayed correctly, it means that the whole streaming path is ready. When the conference data is sent, the message automatically goes away.

Note that the default pre-connection message is an empty string (nothing is displayed).

To create a message in Windows NT 4.0:

- Open the Control Panel from the Start Menu.

- Open the Multimedia applet.

- Click the ‘Devices’ tab.

To create a message in Windows 2000:

- Open the Control Panel from the Start Menu.

- Open the Sounds and Multimedia applet.

- Click the Hardware tab.

- Double-Click on the Legacy Video Capture Devices entry.

- Click on the Properties tab.

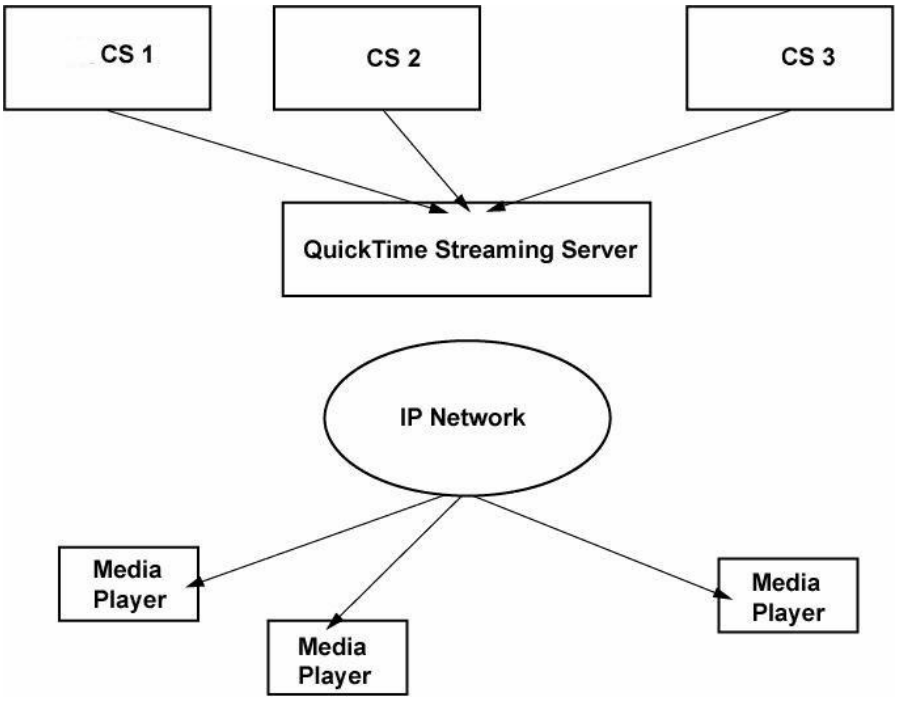
- Select the Stream Video driver, and click the Properties button

Using QuickTime Streaming on the Conference Server

The use of streaming media technology in Conference Server allows the conference to be viewed by large number of viewers across the Internet. To achieve this, usually a streaming server is required in addition to Conference Server to manage the media distribution and client connection control. Some of the popular streaming servers and media players do not support H.323 media format so a streaming media agent (drivers) and encoder are needed to transcoding the conference media. While this transcoding allows the H.323 media available to a vast audience, it does slow down the delivering speed and increases the cost of streaming by adding additional hardware (usually a dedicated high end PC for transcoding). This results in undesirable latency for environments that require near real-time delivery. For the environment that requires low latency Conference Server streaming media delivery, Conference Server supports QuickTime® streaming from Apple Computer®. QuickTime streaming allows for live delivery of H.323 media so there are no transcoding penalties.

As shown in the following figure, Conference Servers send media streams to a QuickTime Streaming Server. The streaming server sends streams to clients (unicast) or network (multicast). The QuickTime player decodes the streams so that the media players are able to play them back.

Figure: Conference Servers and QuickTime Server



Note:

- When (QuickTime) media players are connected directly to the Conference Server without the intervention of the streaming server, the Conference Server will not have the same quality control over streaming media connections as if using the QuickTime Streaming Server, but Conference Server will deliver the specified media to the player in the format of RTP packets. This connection is completely configured through the SDP file opened through the media player.
- If you have multiple Conference Servers, you need either multiple streaming servers or need to specify different ports in a single streaming server. Multiple SDP files are required to specify these different ports.

To prepare for Conference Server QuickTime streaming, you need to complete the following procedures:

1. **Install and start QuickTime Streaming Server and player**

   To install QuickTime Streaming Server and player, please refer to the related documents provided by the manufacturer (Apple Computer) or visit the appropriate Web site. Before you install, make certain that you have the correct OS and other system requirements for the product.

2. **Prepare the media source**

   - Start Conference Server and login as an administrator.
   - Create a H.323 conference and set the audio format to G.711u, set the video format to H.261, and set this conference streaming to the streaming server.
   - Proceed to connect the clients into the conference.

3. **Prepare the streaming server**

   - Make any necessary changes to the streaming server's configuration file. For the Darwin streaming server, it is called **streamingserver.cfg**. If any changes are made to the configuration file, you will need to restart the streaming server to make those changes take effect.
   - Verify that the streaming server will function properly before streaming by using the sample movie file provided by the streaming server.

     For example, you can start Darwin Streaming Server and start the QuickTime player. On QuickTime player, select the menu item: **File->Open URL…**and enter the URL in the following format:

     ```
     rtsp://<the ip address of streaming server>/<sample movie file>
     ```

     If you changed the default **rtsp port** in the streaming server configuration file, you have to specify the port in your URL, like this:

     ```
     rtsp://<ip address of streaming server>:<port>/<sample movie file>
     ```

     For example, if you have the streaming server at **10.1.1.100** using rtsp port **664** and select the movie file called **sample.mov** in the movie folder, you can use the following URL in your QuickTime player:

     ```
     rtsp://10.1.1.100/sample.mov
     ```

     After successfully playing the sample movie, continue to the next step.

4. **Prepare the streaming server for live streaming**

The QuickTime media player delivers live streaming is by connecting to a streaming server using Session Description Protocol (SDP). SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. You need to create an SDP file for your streaming session.

Creating an SDP file

To enable the Streaming Server to do live streaming, a Session Description Protocol (SDP) file needs to be created.

A summary of the commonly used SDP descriptions is listed below (optional items are indicated by an '*'):

v

protocol version

o

owner/creator and session identifier

s

session name

i*

session information

u*

URL of description

e*

e-mail address

p*

phone number

c*

connection information – not required if included in all media

b*

bandwidth information

z*

time zone adjustments

k*

encryption key

a*

zero or more session attribute lines

t

time the session is active

r*

zero or more repeat times

m

media name and transport address

For example, a session is set up with a Conference Server conference at IP address **10.1.1.111** and a QuickTime Streaming Server at IP address **140.249.44.112**. This session is set to start immediately when the player gets connected and the player will end the session manually. You can create a SDP file similar to the following example:

```
v=0
o=xman 30701 IN IP4 10.1.1.111
s=my stuff meeting
c=IN IP4 10.1.1.112
t=3194197982 0
m=audio 1424 RTP/AVP 0
m=video 1414 RTP/AVP 31
```

Use the default SDP file skeleton, **default.sdp**, to create your own custom SDP file.

Make your changes based on this file.

SDP Creation Tool

There is also a web-based tool to create an SDP file based on your input. An SDP creation tool, the SDP page, is a web-based tool, easily accessible with a Web browser and network connection, used to create an SDP file. It is also based on a template, so it is easier to customize and localize to your needs.

Installation

The SDP page should be installed by the Conference Server, or by an MCC installer. Otherwise, put the csqt.war file under the <tomcat_home>\webapps directory and restart Tomcat to automatically install it. Next, you need to configure the SDP page before it can be used.

Configuration File

The configuration file is located at **<tomcat_home>\webapps\csqt\conf** and the file name is **sdp.properties**. This text file can be edited it using any text editing tool. The sdp.properties file contains the following items:

ConfDir

This is the directory of the streaming server configuration file, see below

ConfigFile

This is the file name of the streaming server configuration file. Default: **streamingserver.cfg**

MovieFolder

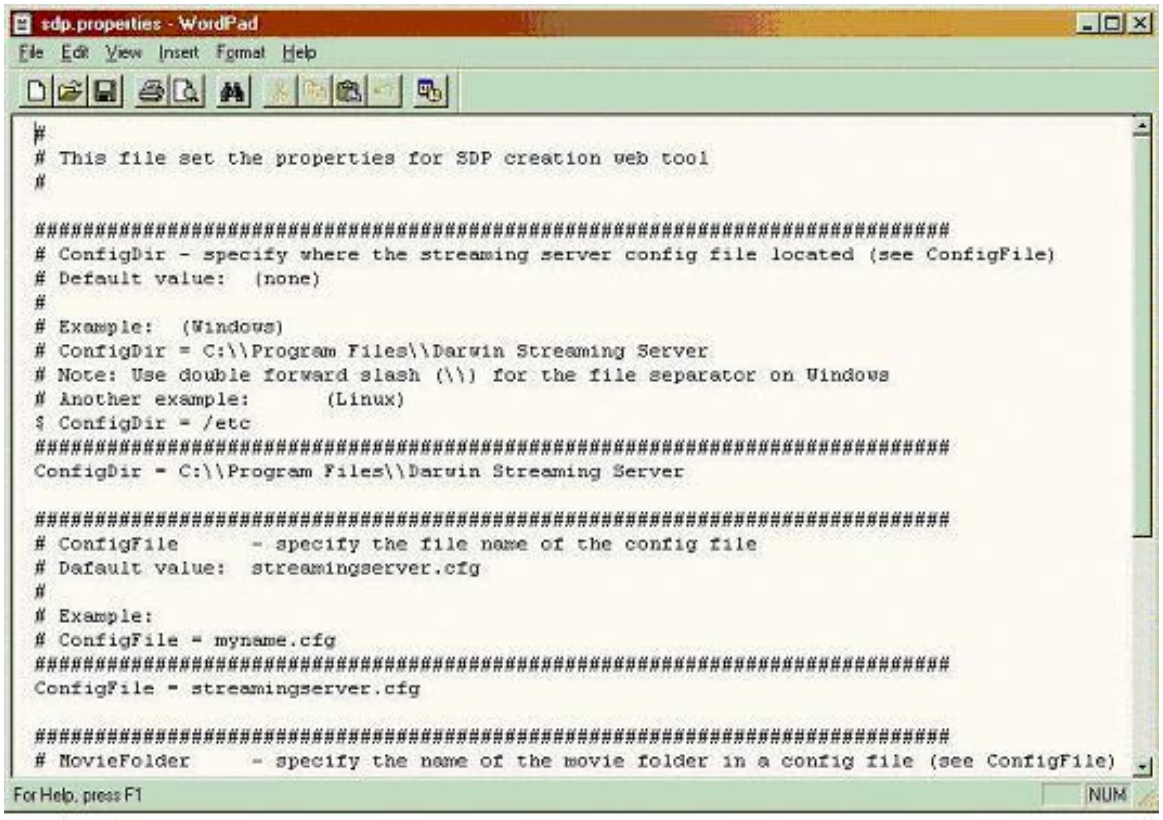
This is the directory name of the movie folder. Default: **movie_folder**

TemplateFile

This is the file name of the SDP page template file. Default: **template.xml**

The following figure shows an example of the sdp.properties file:

Figure: The SDP Properties File


sdp.properties - WordPad
File Edit View Insert Format Help
#
This file set the properties for SDP creation web tool
#
ConfigDir - specify where the streaming server config file located (see ConfigFile)
Default value: (none)
#
Example: (Windows)
ConfigDir = C:\\Program Files\\Darwin Streaming Server
Note: Use double forward slash (\\) for the file separator on Windows
Another example: (Linux)
$ ConfigDir = /etc
ConfigDir = C:\\Program Files\\Darwin Streaming Server
# ConfigFile - specify the file name of the config file
# Default value: streamingserver.cfg
#
# Example:
# ConfigFile = myname.cfg
ConfigFile = streamingserver.cfg
# MovieFolder - specify the name of the movie folder in a config file (see ConfigFile)
For Help, press F1
NUM

Note: For the latest version of the Web SDP application, if you do not have the streaming server installed on your system, you can still use this tool to create an SDP file. The default location for the created SDP file will be at the same **conf** directory instead of the **movie_folder** of the streaming server.

Using the SDP Page

To access the SDP page:

- Type in the following URL into your Web browser:

  `http://<ip_of_streaming_server>:<port>/csqt/sdp`

  Note: Tomcat must be running on the system of streaming server.

  For example, if the IP address of the Streaming Server is **10.1.1.100** and the default port **8080** is used, after typing in the URL and loading the page, the login page will display.

- Enter csqt as the user name and changeme as the password. Then click OK to bring you to the SDP Session File Creation Page.
- The main page of the SDP file lists the templates that the file, template.xml, contains. It also gives a short description of each template session, so you can choose a session that best suits your needs.
- Follow the link to enter and confirm the data for that session. This will display data input page.
- Read the instructions and enter data into the text fields marked as required. If no information

is entered, the file will be built.

- Fill in the session text box. This is the file name to be created. Make sure to use sdp as the file extension. If you create the same file twice, the first file will be overwritten. Select a different file name if you want a separate file.
- Fill In the following text fields:
    - **session:user -** enter the name of the user
    - **session:id -** enter a unique session id for each sessions running
    - **session:ip -** enter the IP address of the Conference Server
    - **connection:ip -** enter the IP address of the streaming server
    - **name -** enter the name of the session
- Double-check the time format. Use the default value as a reference. It the stop_time is zero, then this session is not time-bound. The session will continue until is manually.

  Port: enter the port number if it has been changed from the default value in Conference Server streaming.
- After completing the required fields, click the build button. A confirmation page will display that will state that the SDP file is being saved to the movie folder, or an error page will display requiring you to re-enter the some of the data. You may either logout or return to the main page.

Login and Logout

To use the SDP page, you have to login as an administrator. The default users are **Admin** and **tomcat**. If you want another user group to use the SDP page, contact your Tomcat administrator or refer to the Tomcat documentation for instructions about how to manage users.

After logging out from the SDP page, you need to re-login to use it again. If you do not want users to use the **Back** button to view the SDP page, delete the cached pages in your Web browser.

Using SNMP with the Conference Server

The Conference Server includes dynamic services such as SNMP and SOAP. These services are user-configurable through the **svc.conf** file.

By default, SNMP is enabled on the Conference Server at start-up. But you can decide whether the corresponding library is loaded or not. Once the svc.conf is modified, you must re-start the Conference Server to make your changes take effect.

Where is the service configuration file?

On Windows, the **svc.conf** file is located in **<SysDir>/system32**. On Linux/Solaris, it is located in **<InstallDir>/<YourMachineName>.**

How do you modify the service configuration file?

The svc.conf file contains a brief name description for each service that can be used by the Conference Server. For example:

```
#Enable the Loadable Loadable Service
```

is followed in the next line by a configuration command.

If you want a service to be dynamically loaded, remove the leading comment sign (#) of the configuration command.

```
dynamic LS_SNMP Service_Object * UscsSnmp:_make_UscsSnmpEntry() ""
```

You can change this line to add the initialization parameters for the service. For example, to use 10082 as the HTTP port for the Conference Server SOAP, the configuration command is:

```
dynamic LS_SOAP Service_Object * UscsSoap:_make_UscsSoapEntry() "-p
10082"
```

If you no longer need a service, add the leading comment sign (#) to the configuration command.

```
#dynamic LS_SNMP Service_Object * UscsSnmp:_make_UscsSnmpEntry() ""
```

SNMP Support

Click to Meet Conference Server supports Simple Network Management Protocol (SNMP). The Conference Server implements the H323MC-MIB protocol as defined by H.341 Annex A.

For information on how to configure the SNMP dynamic service, see Configuring Dynamic Services.

The SNMP agent supports both MIBII and H323MC-MIB. For more information, see the Conference Server release notes at http://support.clicktomeet.com. Follow the link to support.

Configuring the SNMP Agent from a Windows System

By default, the Conference Server installation wizard installs the SNMP agent (snmps 7.x.x). SNMP is a Windows service, so you can configured it to start manually or automatically.

On Windows, the agent configuration file (**snmps.conf**) is located in the same directory as the SNMP agent. You can find the path from the Windows registry string 'ImagePath' at:

[\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\snmps 7.x.x].

The default is the same directory as the Conference Server. On Linux/Solaris, it is located at:

<InstalledDir>/<YourMachineName>.

You can edit the configuration file to meet your needs. Note that if you have another SNMP service running on the same system, you have to stop the other service before you can start the Conference Server service.

Configuring the SNMP Agent from a Unix System

The Conference Server installation wizard installs the SNMP agent (snmpd) by default. On Unix systems, the SNMP agent is a daemon program. Use the following commands with the snmpd agent:

- To start the agent - #/etc/init.d/snmpd start
- To stop the agent - #/etc/init.d/snmpd stop
- To restart the agent - #/etc/init.d/snmpd restart

The configuration file (**snmpd.conf)** is located at **<InstallDir>/<HostName>/ directory**. You can edit the configuration file to meet your needs. Note that if you have another SNMP agent daemon running on the same system, you have to stop the other before you can start Conference Server's.

The SNMPD.conf file

The snmpd.conf is the default configuration file for the SNMP agent. The following paragraph shows the most important sections of the configuration file. The file is also well annotated with many commented-out examples.

The following sections are related to change the access control:

- **Community section** - Maps the community name (COMMUNITY) to a security name (local or other), depending on where the request comes from:

#	**sec.name**	**source**	**community**
com2sec	me	default	yourname
com2sec	local	localhost	private
#com2sec	mynetwork	123.4.5.0/24	myteam
#com2sec	notConfigUser	default	public

- **Group section** - Maps the security names to group names:

#		**sec.module**	**sec.name**
group	group1	v1	me
group	group1	v2c	me
group	group1	usm	me
group	MyRWGrp	v1	local
group	MyRWGrp	v2c	local
group	MyRWGrp	usm	local
#group	MyROGrp	v1	mynetwork
#group	MyROGrp	v2c	mynetwork
#group	MyROGrp	usm	mynetwork
#group	notConfigGrp	any	notConfigUser

- **View section** - Creates a view to let the group have rights to:

#		**incl/excl**	**subtree**	**mask**
view	sysview	included	.1.3.6.1.2.1.1	
view	h323Mc	included	.0.0.8.341.1.1 .4	
view	all	included	.1	80

- **Access right section** - Gives a group access rights to a view:

#context	**sec.model**	**sec.level**	**match**	**read**	**write**	**notif**
group1	""any	noauth	exact	all	all	all
MyRWGrp	"" any	noauth	exact	all	all	none

MyROGrp	"" any	noauth	exact	h323Mc	h323Mc	none
#notConfigGrp	"" any	noauth	0	sysview	none	none

Using SOAP with the Conference Server

The Conference Server includes a dynamic service that provides a programming interface that uses SOAP. The user can send telnet commands and choose to receive telnet events from the Conference Server using the SOAP interface. The Conference Server 7.x SOAP supports WSDL 1.0 and SOAP 1.1.

The HTTP port used by the Conference Server SOAP is configurable by using -p <port> as an initialization argument in svc.conf file. For information on how to configure the SOAP dynamic service, see Configuring Dynamic Services.

The URL for a remote SOAP client to connect to the Conference Server is:

http://<ConferenceServerIP>:<port>

Use 10080 for the default <port> value.

For example, if your Conference Server is installed at IP address 1**23.4.5.6**, the URL would be:

http://123.4.5.6:10080

Use the localhost as the <ConferenceServerIP>. The client in the preceding example is running on the same machine as the Conference Server.

Note: SOAP clients outside the firewall cannot receive SOAP telnet events from the Conference Server. Be sure to check the release notes for the most recent information about the SOAP API.

The following is the complete description of the Conference Server SOAP interface in WSDL format.

```
<?xml version="1.0"?>
<definitions targetNamespace="http://www.clicktomeet.com/server"
     xmlns="http://schemas.xmlsoap.org/wsdl/"
     xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
     xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
     xmlns:tns="http://www.clicktomeet.com/server"
     xmlns:xsd2="http://www.clicktomeet.com/server/schema"
     xmlns:xsd="http://www.w3.org/2000/10/XMLSchema">

     <annotation>
          <author> Jason Danielson </author>
          <date>2003-07-25</date>
          <documentation>This is the definition of the
          Server</documentation>
     </annotation>

     <message name="sendTelnetCmdRequest">
          <part name="cmd" type="xsd:string"/>
     </message>
     <message name="sendTelnetCmdResponse">
          <part name="result" type="xsd:string"/>
     </message>
     <message name="sendTelnetEventRequest">
```

```
     <part name="event" type="xsd:string"/>
</message>
<message name="sendTelnetEventResponse">
     <part name="result" type="xsd:integer"/>
</message>

<portType name="Server">
     <operation name="sendTelnetCmd">
          <input message="tns:sendTelnetCmdRequest"
                 name="sendTelnetCmd"/>
          <output message="tns:sendTelnetCmdResponse"/>
     </operation>
</portType>

<portType name="Client">
     <operation name="onTelnetEvent">
          <input message="tns:sendTelnetEventRequest"
                 name="sendTelnetEvent"/>
          <output message="tns:sendTelnetEventResponse"/>
     </operation>
</portType>
<binding name="ServerSOAPBinding" type="tns:Server">
     <soap:binding style="rpc"
          transport="http://schemas.xmlsoap.org/soap/http"/>
     <operation name="sendTelnetCmd">
          <soap:operation
             soapAction=
              "http://www.clicktomeet.com/server/sendTelnetCmd"
             style="rpc"/>
          <input>
               <soap:body
                    encodingStyle=
                    "http://schemas.xmlsoap.org/soap/encoding/"
                    namespace=
                    "http://www.clicktomeet.com/server"
                    use="literal"/>
          </input>
          <output>
               <soap:body
                    encodingStyle=
                    "http://schemas.xmlsoap.org/soap/encoding/"
                    namespace=
                    "http://www.clicktomeet.com/server"
                    use="literal"/>
          </output>
     </operation>
</binding>
<binding name="ClientSOAPBinding" type="tns:Client">
     <soap:binding style="rpc"
          transport="http://schemas.xmlsoap.org/soap/http"/>
     <operation name="onTelnetEvent">
          <soap:operation
             soapAction=
              "http://www.clicktomeet.com/server/onTelnetEvent"
             style="rpc"/>
          <input>
               <soap:body
```

```
                    encodingStyle=
                    "http://schemas.xmlsoap.org/soap/encoding/"
                    namespace=
                    "http://www.clicktomeet.com/server"
                    use="literal"/>
               </input>
               <output>
                    <soap:body
                    encodingStyle=
                    "http://schemas.xmlsoap.org/soap/encoding/"
                    namespace=
                    "http://www.clicktomeet.com/server"
                    use="literal"/>
               </output>
          </operation>
     </binding>
     <service name="ClickToMeetSoapTelnet">
          <port binding="tns:ServerSOAPBinding" name="Server">
               <soap:address
                  location=
                  "http://localhost:10080/clicktomeet/7.4/server/"/>
          </port>
          <port binding="tns:ClientSOAPBinding" name="Client">
               <soap:address
                  location=
                  "http://localhost:10081/clicktomeet/7.4/client/"/>
          </port>
     </service>
     <types>
          <schema
          targetNamespace="http://www.clicktomeet.com/server/schema"
               xmlns:xsd2="http://www.clicktomeet.com/server/schema"
               xmlns="http://www.w3.org/2000/10/XMLSchema">
               <element name="strVector">
                    <complexType>
                         <sequence>
                              <element type="string"/>
                         </sequence>
                    </complexType>
               </element>
               <complexType name="intVector">
                    <sequence>
                         <all>
                              <element type="integer"
                              nullable="true"/>
                         </all>
                    </sequence>
               </complexType>
               <complexType name="ArrayOfInt" base="soap:Array">
                    <sequence>
                         <element name="x"
                              type="xsd:integer"
                              maxOccurs="unbounded"/>
                    </sequence>
               </complexType>
               <element name="GetErrorMsg">
                    <complexType>
```

```
                    <all>
                        <element name="errorMsg"
                        type="string"/>
                    </all>
                </complexType>
            </element>
            <element name="ints" type="xsd2:ArrayOfInt"
            nullable="true"/>
        </schema>
    </types>
</definitions>
```

Working with Conference Server's Historical Statistics

You can choose to have Conference Server log statistical information concerning activity on your Conference Server to a file called (optionally) **cs.stats.** The information Conference Server logs to this file can be used for network capacity planning, cost analysis, and more**.** Conference Server formats cs.stats as a comma delimited file that you can import into a standard text editor or spreadsheet application for graphing and interpretation (see the following figure).

cucs.stats

	A	B	C	D	E	F	G	H
1	Mon Sep 25 17:04:00 2000							
2	Time	Conf	MB Processed	MB Pruned	Avg. Users	Tot. Time	Cur. Users	Connects
3	17:04:00	0	24.87	0	7	210.23	15	69
4	17:04:00	1	0.9	0	7	205.78	15	45
5	17:04:00	2	0.62	0	6	159.33	9	73
6	17:04:00	3	0.31	0	3	94.88	6	24
7	17:04:00	4	5.21	0	1	49.4	3	14
8	17:04:00	5	0	0	0	0.17	0	1
9	17:04:00	33	0	0	0	0	0	0
10	17:04:00	44	23.02	0	2	29.72	3	3
11	Mon Sep 25 17:19:05 2000							
12	Time	Conf	MB Processed	MB Pruned	Avg. Users	Tot. Time	Cur. Users	Connects
13	17:19:05	0	56.77	0	8	270.55	13	19
14	17:19:05	1	1.04	0	8	250.22	12	17
15	17:19:05	2	0.87	0	8	231.45	12	34
16	17:19:05	3	0.41	0	4	126.82	8	15
17	17:19:05	4	5.61	0	2	49.87	4	6
18	17:19:05	5	0.2	0	0	1	0	2
19	17:19:05	33	0	0	0	0	0	0
20	17:19:05	44	22.27	0	1	53.75	2	2

cucs.stats

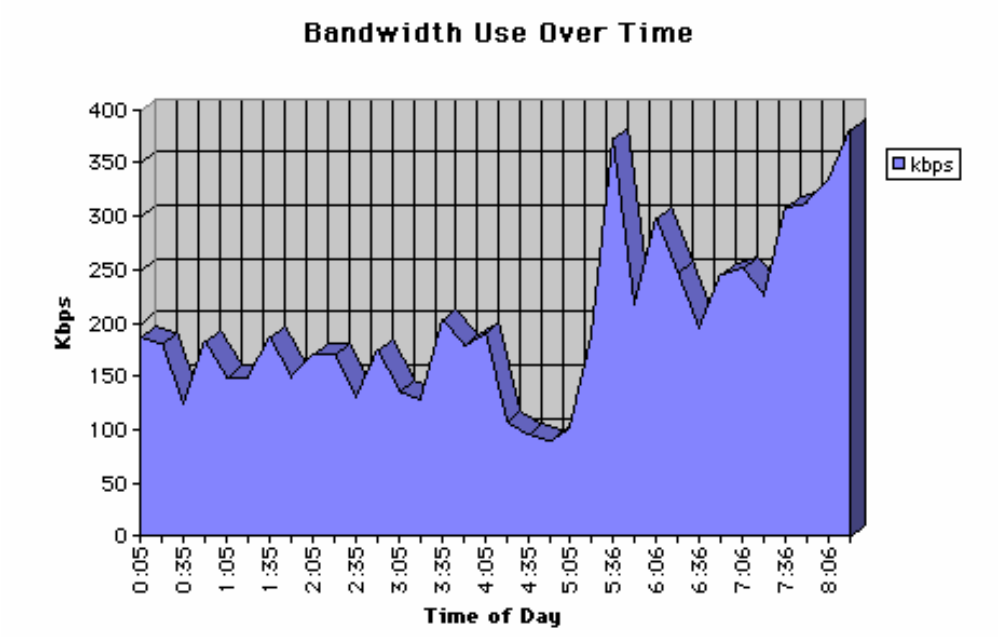
Conference Server logs statistical data to a single file for your entire server. You determine the parameters for this file when you add a Conference Server to your Conference Server domain (see Historical Statistics). If there are multiple Conference Servers in your domain, each will keep its own cs.stats log file.

In the log file, Conference Server provides statistical data in a number of categories for each conference on your server. These categories are:

- Megabytes of data the Conference Server processed since the last date/time stamp
- Megabytes of data the Conference Server pruned since the last date/time stamp (intelligently discarded because of bandwidth limitations)
- Average number of participants connected since the last date/time stamp
- Total active time since the last date/time stamp (total number of participants multiplied by total amount of connect time for all participants)
- Number of participants connected at the time of the date/time stamp

- Total number of connections made to the server since the last date/time stamp

Once you import this statistical data into a spreadsheet application, you can manipulate it in many different ways, depending on your needs. You can look at the information per conference, per server, as a single interval of time, or as a time series. For example, a network service provider may want to track bandwidth used by videoconferencing participants over time (see the following figure). This information would show peak hours of use and help the provider in network capacity planning.



The same provider may want to track the total number of participants and average connect time in a particular conference. This information could help measure the success of an interactive event. A system administrator managing a busy corporate network may want to look at videoconferencing traffic for a particular slice of time in order to map it to network performance. This information could help the administrator set appropriate limits on maximum number of participants allowed on the server simultaneously, and on client send/receive rates for Conference Server conferences.

These are but a few examples of how Conference Server's statistical data can be used. There are many more. The purpose of the stats log file is to provide the raw data that you can, in turn, use for your own analysis.

Simple Cascading

Simple cascading enables the Conference Server to send media between several servers. Each server in the simple cascading configuration acts as an endpoint. Using unicast, the media flow s appropriately between multiple servers in mixed audio and switched video streams.

Cascading is beneficial because:

- Cascading servers increase the number of participants a conference can accommodate. The number users in a conference can be greater than the total number licensed users for any one Conference Server. With cascading, the conference maximum is the total of licensed user on all cascaded Conference Servers *combined*.
- Simple H.323 cascading reduces bandwidth between the servers by having each server mix audio locally and send the mixed stream to the other servers. This allows the local

servers on each LAN segment to minimize the WAN communication.

- Cascaded servers can take advantage of Quality of Service (QOS) on the Cisco MCM gatekeeper. This allows you to guarantee QOS for a distributed conference
- When video is enabled, only one video stream is sent between cascaded servers. This minimizes server traffic.

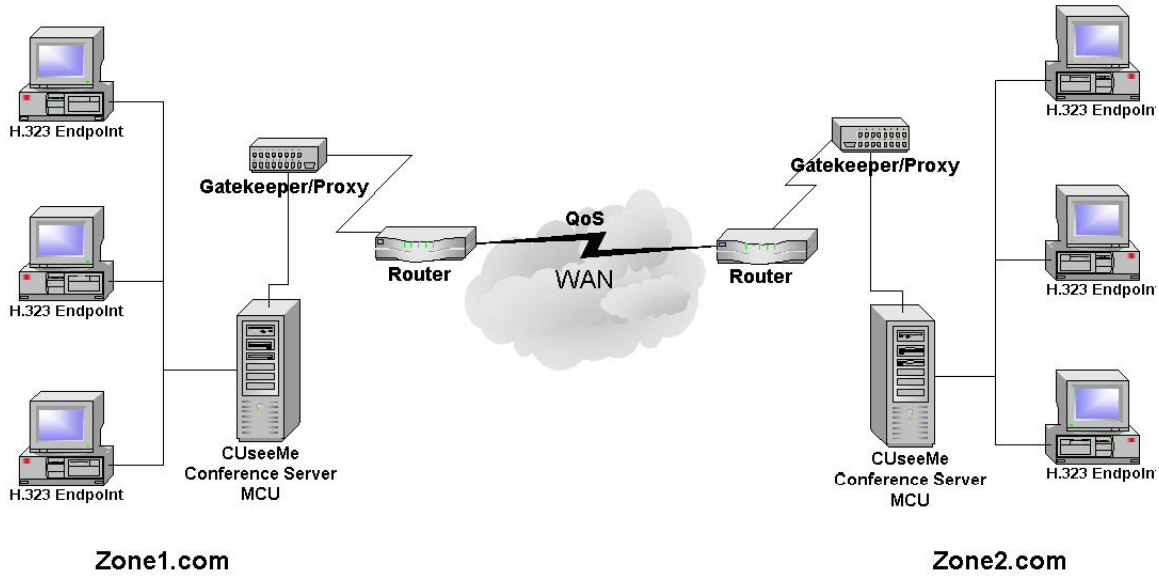
Do not set up simple cascading if:

- You cannot use the Conference Server (MCU) per user controls on other MCUs. You do not know who is on the other MCU; you just get the mixed audio of everyone and the switched video the MCU chooses. Intelligent Linking lets any audio or video be sent between the MCUs as well as all the user information.
- You cannot use simple cascading with Continuous Presence because the combined CIF output is not accepted as a QCIF stream on other Conference Servers. Intelligent Linking lets each Conference Server receive the four separate QCIF streams and mix them on each Conference Server.

Setting up Simple Cascading

The following are instructions for configuring two servers, each registered with different gatekeepers. In this scenario, the gatekeepers are in different zones.

The Administrative GUI centrally manages the servers in this example.



1. Configure the two servers as members on the Administrative GUI Network page.
2. Set their respective H.323 domain names and register them with their gatekeepers.

   In this example, each Conference Server registers with a different gatekeeper and each gatekeeper manages its own zone. For example, Zone1.com is the H.323 domain name of the server with which the gatekeeper is registered.
3. Set up a similar configuration for the other Conference Server. In our example, the other server registers with a different gatekeeper using the H.323 domain name of Zone2.com.
4. Create a conference using the Administrative GUI's Conferences page.

   The Conference Nickname in the Conference Aliases section is conf00002@Zone1.com. The H.323 domain name of the conference is appended to the conference nickname. You can change the default conference nickname, but it is not necessary in this example.
5. Define the server layout for the conference.

   In this example, both servers are added to the conference layout. It is not necessary to link the servers, as this creates a intelligent link instead of simple cascading. The actual cascading is initiated later.

   Any server in the layout of a conference also creates that conference. For example, the second server creates a conference with a nickname of conf00002@Zone2.com.
6. To cascade the conferences, use the CallOut Applet to invite conference 2 from the server at Zone2 into conference 2 in Zone1.

The servers now send each other mixed audio and switched video. They also take advantage of QOS on the the network and gatekeeper.

Both servers display as endpoints, or participants, in the other's conference on the Monitor Users page.

What if there are two servers registered to the same gatekeeper?

The previous example worked because the gatekeepers managed different zones. If the servers are registered to gatekeepers in the same zone, or if they are registered to one gatekeeper, the conference nickname must be unique. This is because the H.323 domain name will be the same for all servers.

You must create the conferences individually on all the servers, and the conference nickname must be unique on each server. As with this example, one server can then cascade with another server by using the CallOut Applet and the conference nickname.

Corporate Web Site

You can find additional information about RADVISION products on our Web site.

- For the latest news from RADVISION, visit http://www.radvision.com/
- **Click to Meet Release Notes** - You can access the Release Notes at http://support.clicktomeet.com. Release Notes contain critical information. It is recommended that you read the release notes prior to installation.
- For access to our database of Frequently Asked Questions (FAQs) and other information, visit: http://support.clicktomeet.com/

Technical Support

RADVISION provides live technical support to our distributors, resellers, and service-contracted customers. If you have purchased your RADVISION product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues. If you need further assistance, please visit the RADVISION Click to Meet web site (http://support.clicktomeet.com).

Third-party Licensing

LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
```

```
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
```

```
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

Index

accessing Conference Server's User Authentication Web page 88
accessing MeetingPlanner 111
adding a conference 51
adding a Conference Server to the Conference Server domain 17
adding user records 28
additional audio 10
address translation 13
administrative server 101
administrator permission 83
admissions control 13
admit reject message 90
admitted senders 54
assigning special permissions 82
audio codecs 39, 63
Delta-Mod 63
DigiTalk 63
G.711 39
G.723 39
Intel DVI 63
Siren 14 63
Siren 7 63
audio latency 65
automatic bandwidth controls 42
avoiding Conference Server layout conflicts 80
backing up the Conference Administrator database 28
backup files 28
bandwidth controls 13, 58
bandwidth detection 42
bandwidth pruning 42
basic settings 52
bidirectional link tool 73
billing architecture 120
billing systems 120
broadcast mode 54
CallOut applet 47
clearing video source 83
codecs 39
audio 39
video 39
Conference Administrator database
defining 26
conference aliases 65
conference attributes 53
conference greeting 53
conference ID 52
conference Manager permission 84
conference name 53
conference owner information 56
conference password 47, 57
conference Server authentication 62
Conference Server tool 73, 74
Conference Server's User Authentication Web page 87
conferences area 49
configuring dynamic services 131
configuring T.120-based conferences 37
Continuous Presence Mode 10
copying a conference configuration 71
copying user records 31
creating a Conference Server layout template 79
creating an SDP file 127
cucs.cur 120
cucs.log 16
cucs.sdf 120
cucs.stats 119
CUseeMe Web 10
customizing the User Authentication Web page 90

data collaboration for non-H.323-based conferences 62
data conferencing with Conference Server's T.120 server 32
default conference routing 47
defining a server layout for your conference 74
defining your RADIUS server 122
denying a user 95
disconnecting a user 94
duration 57
dynamic services
configuring 131
E164 terminal aliases 18, 45
editing a conference configuration 70
editing a Conference Server's settings 25
editing user records 30
enable tracking 69
enabling streaming of a Conference Server conference 123
Enabling T.120
For H.323-based conferences 37
entering a conference password 47
firewalls 21
gatekeeper
monitoring activity 98
gatekeeper functionality 13
gatekeeper settings 18
gatekeepers 13
gateways 13
general user permission 84
admit permission 85
admitted-sender permission 85
deny permission 85
normal permission 84
granting the floor to a user 95
H.263+ Annexes 70
H.323 conferences 13, 39
H.323 VideoSwitcher applet 39
H323 10
H323-ID terminal aliases 18, 45
historical statistics 119
hosting H.323 conferences 13, 39
initializing the Conference Administrator database 28
interfacing with third-party billing systems .. 120
International Telecommunication Union (ITU) 13, 39
Internet Engineering Task Force (IETF) 56
Local Area Network (LAN) 37, 43
log display window 16
log file backup interval 119
log file line limit 119
log file name 119
log interval 119
log out button 16
lurkers 54
managing bandwidth 42
managing organizations 27
manual bandwidth controls 42
setting conference specific limits 42
setting server-wide limits 42
maximum participants 55
MeetingPlanner applet 56
moderator permission 83
monitoring area 91
monitoring dynamic statistics for a conference 97
monitoring dynamic statistics for a Conference Server 98
monitoring gatekeeper activity 98
monitoring users 92
multicast 43, 66, 68
Multicast Backbone (MBONE) 74
multicast tool 73
multiple server conferences 43
Multipoint Control Unit (MCU) 13

NetMeeting 47
optional/advanced settings 55
port number 74
preferred/required codecs 63
private 52
product components 10
Conference Administrator Web Pages 10
Conference Server User Tools 10
Continuous Presence Mode applet 10
H.323 CallOut applet 10
H.323 VideoSwitcher applet 10
MeetingPlanner 10
T.120 server 10
User Authentication Web Page 10
product options 11
additional audio 10
Continuous Presence Mode 10
H323 10
SIP 10
streaming media 10
video 10
providing Conference Server User Tools to client end users 119
Q.931 facility messages 45
QuickTime Streaming 125
RADIUS accounting port 122
RADIUS authentication 63, 90
RADIUS server 122
RADIUS server IP address 122
RADIUS server port 122
receiving video and audio 39
Registration Admission Status (RAS) 13, 47
Remote Authenication Dialing Service (RADIUS) 120
removing a conference 71
removing a Conference Server 21
removing user records 31
repeat conference 58
revoking the floor from a user 96
root 68
scheduling 48
sdf file extension 120
SDP file
creating 127
searching user records 30
selecting a conference 45
selection tool 73
self-reflect 68
setting video source 83
shutting down a Conference Server 21
SNMP 132
SOAP 134
start date 57
start time 57
streaming 70
streaming media 10
synchronizing Conference Server domain members 24
T.120
For H.323-based conferences 37
For non-H323-based conferences 38
T.120 configuation file 33
T.120 server 12, 32, 46
T.120 standard 12
T.120 throughput enforcement 35
TCP port 37
technical support 141
template conference 56
terminal aliases 18, 45
E164 ..... 18, 45
H323-ID 18, 45
terminals 13
third-party billing systems 120
Through a gatekeeper 45
Through default conference routing 47

Through the H.323 CallOut applet 47
Through the T.120-based server 46
Through the User Authentication Web page 46
time limits 62
time to live (TTL) 68
top provider tool 73, 74
UDP port 37
understanding Conference Server's billing architecture 120
understanding the T.120 standard 12
understanding unicast and multicast 66
unicast 43, 66
unidirectional link tool 73, 74
User Authenication Web Page 46, 120
user authentication 62, 90, 120
user identifier fields 29
user tools 119
users 83
adding 28, 83
copying 31
denying 83
disconnecting 83
editing 30
granting floor to 83
managing organizations 27
revoking floor from 83
users area 82
using and accessing the monitoring area as a moderator 91
using Conference Server's CallOut applet . 106
using Conference Server's Continuous Presence Mode applet 102
using Conference Server's H.323 VideoSwitcher applet 104
using MeetingPlanner with conference manager permission 114
using MeetingPlanner with general user permission 112
using the Monitoring area as an Administrator 91
using the SDP page 130
video 10
video codecs 39, 58, 64
Cornell CuseeMe Gray 64
CUseeMe Networks Color 64
CUseeMe Networks M-PEG 64
H.261 ..... 39, 58
H.263 ..... 39, 58
H261.CIF 39, 58
H261.CP4 58
H263 Annex F 64
H263 Annex P5 64
H263.CIF 58
H263.QCIF 58
H263.SQCIF 58
video source setting 97
video switching 39
videoconferencing server 10
viewing available conferences 49
what is Conference Server? 10
whiteboarding 12
Wide Area Network (WAN) 37, 43
working with Conference Server's historical statistics 137
working with firewalls 21
working with the conference administrator database 26
working with the Conference Administrator Web pages 15
working with the Conference Server layout applet 73
zone management 13